Guide de l’utilisateur

AWS Accès vérifié

AWS Accès vérifié: Guide de l’utilisateur

Table of Contents

Qu'est-ce que l'accès AWS vérifié ?

Avec AWS Verified Access, vous pouvez fournir un accès sécurisé à vos applications sans avoir à utiliser un réseau privé virtuel (VPN). Verified Access évalue chaque demande d'application et permet de garantir que les utilisateurs peuvent accéder à chaque application uniquement lorsqu'elle répond aux exigences de sécurité spécifiées.

Avantages d'un accès à un accès à un

- Posture de sécurité améliorée — Un modèle de sécurité traditionnel évalue l'accès une seule fois et autorise l'utilisateur à accéder à toutes les applications. Verified Access évalue chaque demande d'accès aux applications en temps réel. Il est donc difficile pour les acteurs malveillants de passer d'une application à l'autre.
- Intégration aux services de sécurité : Verified Access s'intègre aux services de gestion des identités et des appareils, y compris les services tiers AWS et les services tiers. À l'aide des données de ces services, Verified Access vérifie la fiabilité des utilisateurs et des appareils par rapport à un ensemble d'exigences de sécurité et détermine si l'utilisateur doit avoir accès à une application.
- Expérience utilisateur améliorée : Verified Access évite aux utilisateurs d'utiliser un VPN pour accéder à vos applications. Cela permet de réduire le nombre de demandes d'assistance liées à des problèmes liés au VPN.
- Résolution des problèmes et audits simplifiés : Verified Access enregistre toutes les tentatives d'accès, offrant ainsi une visibilité centralisée sur l'accès aux applications, pour vous aider à répondre rapidement aux incidents de sécurité et aux demandes d'audit.

Accès à AWS un accès vérifié

Vous pouvez utiliser l'une des interfaces suivantes pour comment utiliser

- AWS Management Console— offre une interface Web que vous pouvez utiliser pour créer et gérer des ressources d'accès vérifié. Connectez-vous à la AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

- AWS Command Line Interface(AWS CLI) — Fournit des commandes pour un large éventail deServices AWS, y compris l'accès AWS vérifié. La AWS CLI est prise en charge sur Windows, macOS et Linux. Pour obtenir la AWS CLI, consultez AWS Command Line Interface.
- AWSKits SDK — Fournissent des API spécifiques du langage. Les AWS kits SDK prennent en charge la plupart des détails de connexion, notamment le calcul des signatures et le traitement des nouvelles tentatives de demande et le traitement des erreurs. Pour plus d'informations, consultez Kits SDK AWS.
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de requête est le moyen le plus direct d'accéder à un accès vérifié. Toutefois, il faut alors que votre application gère les détails de bas niveau, notamment la génération du hachage pour signer la demande et le traitement des erreurs. Pour plus d'informations, consultez la section Actions d'accès vérifié dans la référence des API Amazon EC2.

Ce guide comment AWS Management Console

Tarification

Vous êtes facturé par heure pour chaque attachement sur Verification et pour le volume de données traité par celle-ci. Pour en savoir plus, consultez Tarification de AWS Verification.

Comment fonctionne l'accès vérifié

AWSVerified Access évalue chaque demande d'application émanant de vos utilisateurs et autorise l'accès en fonction de :

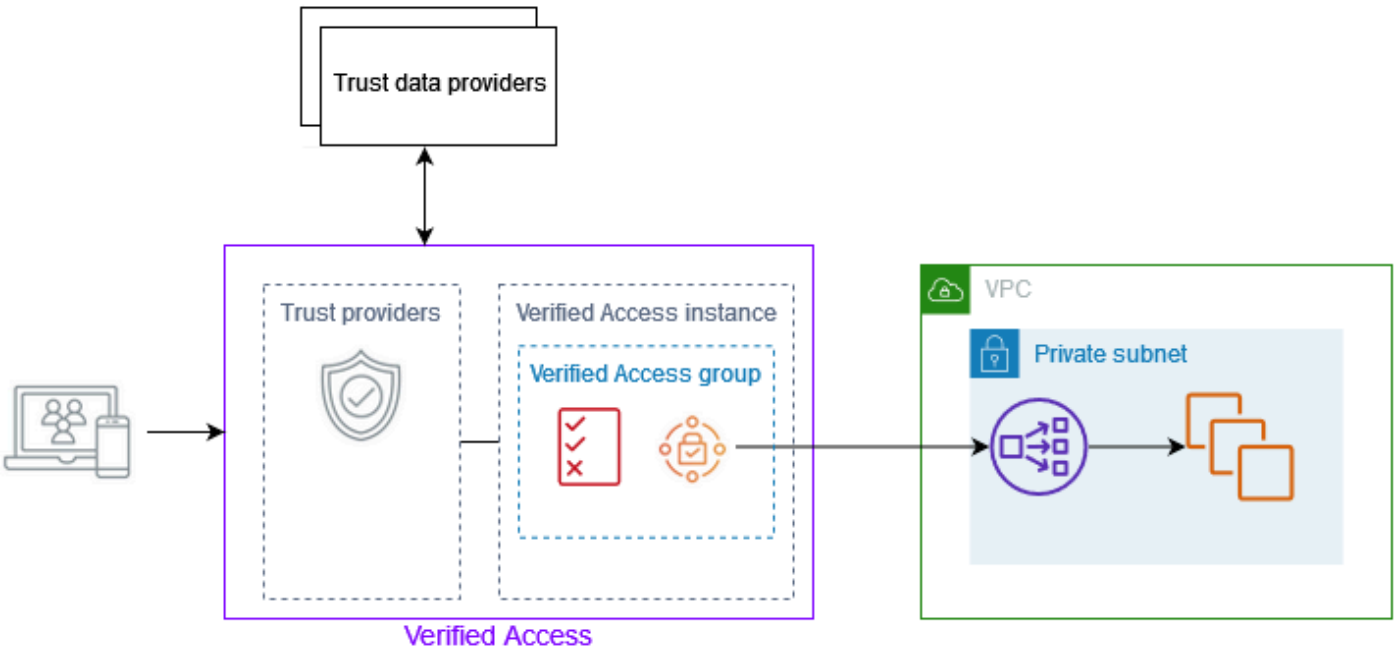
- Données de confiance envoyées par le fournisseur de confiance que vous avez choisi (en provenance AWS ou par un tiers).
- Politiques d'accès que vous créez dans Verified Access.

Lorsqu'un utilisateur essaie d'accéder à une application, Verified Access obtient ses données auprès du fournisseur de confiance et les évalue par rapport aux politiques que vous avez définies pour l'application. L'accès vérifié n'autorise l'accès à l'application demandée que si l'utilisateur répond aux exigences de sécurité que vous avez spécifiées. Toutes les demandes d'application sont refusées par défaut, jusqu'à ce qu'une politique soit définie.

En outre, Verified Access enregistre chaque tentative d'accès pour vous aider à répondre rapidement aux incidents de sécurité et aux demandes d'audit.

Composants clés de Verified Access

Le schéma suivant fournit une vue d'ensemble de haut niveau de Verified Access. Les utilisateurs envoient des demandes d'accès à une application. Verified Access évalue la demande par rapport à la politique d'accès du groupe et à toute politique de point de terminaison spécifique à l'application. Si l'accès est autorisé, la demande est envoyée à l'application via le point de terminaison.



- Instances à accès vérifié : une instance évalue les demandes d'applications et n'accorde l'accès que lorsque vos exigences de sécurité sont satisfaites.
- Points de terminaison d'accès vérifiés : chaque point de terminaison représente une application. Vous pouvez créer un point de terminaison d'équilibrage de charge ou un point de terminaison d'interface réseau.
- Groupe Verified Access : ensemble de points de terminaison Verified Access. Nous vous recommandons de regrouper les points de terminaison des applications présentant des exigences de sécurité similaires afin de simplifier l'administration des politiques. Par exemple, vous pouvez regrouper les points de terminaison de toutes vos applications de vente.
- Politiques d'accès : ensemble de règles définies par l'utilisateur qui déterminent s'il convient d'autoriser ou de refuser l'accès à une application. Vous pouvez spécifier une combinaison de facteurs, notamment l'identité de l'utilisateur et l'état de sécurité de l'appareil. Vous créez une politique d'accès de groupe pour chaque groupe d'accès vérifié, qui est héritée par tous les points de terminaison du groupe. Vous pouvez éventuellement créer des politiques spécifiques à l'application et les associer à des points de terminaison spécifiques.
- Fournisseurs de confiance : service qui gère les identités des utilisateurs ou l'état de sécurité des appareils. Verified Access fonctionne à la fois avec AWS des fournisseurs de confiance tiers. Vous devez associer au moins un fournisseur de confiance à chaque instance d'accès vérifié. Vous pouvez associer un seul fournisseur de confiance d'identité et plusieurs fournisseurs de confiance d'appareils à chaque instance d'accès vérifié.

- Données de confiance : données relatives à la sécurité des utilisateurs ou des appareils que votre fournisseur de confiance envoie à Verified Access. Également appelé « réclamations des utilisateurs » ou « contexte de confiance ». Par exemple, l'adresse e-mail d'un utilisateur ou la version du système d'exploitation d'un appareil. Verified Access évalue ces données par rapport à vos politiques d'accès lorsqu'il reçoit chaque demande d'accès à une application.

Tutoriel : Premiers pas avec Verified Access

Utilisez ce didacticiel pour démarrer avec AWS Verified Access. Vous allez apprendre à créer et à configurer des ressources d'accès vérifié.

Avant d'ajouter cette application à Verified Access, l'application n'était accessible que via votre réseau privé. À la fin de ce didacticiel, des utilisateurs spécifiques peuvent accéder à la même application via Internet, sans utiliser de VPN.

> **Note**
>
> Cet exemple ne montre pas l'intégration avec le fournisseur de confiance basé sur votre appareil. Dans cet exemple, nous travaillons uniquement avec un fournisseur de confiance basé sur l'identité.

Tâches

Prérequis

Les prérequis pour ce didacticiel sont les suivants :

- Pour illustrer cet exemple d'utilisation de l'accès vérifié, nous en utiliserons deuxComptes AWS. Un compte hébergera votre application cible et les ressources d'accès vérifié seront créées dans l'autre compte.
- Activez AWS IAM Identity Center dans Région AWS celui dans lequel vous travaillez. Vous pouvez ensuite utiliser IAM Identity Center en tant que fournisseur de confiance avec Verified Access. Pour plus d'informations, consultez la section Activer le centre d'identité IAM dans le guide de l'AWS IAM Identity Centerutilisateur.
- Un domaine public hébergé et les autorisations requises pour mettre à jour les enregistrements DNS du domaine.
- Une application exécutée derrière un équilibreur de charge interne dans unCompte AWS. L'exemple de nom de domaine d'application que nous allons utiliser est`www.myapp.example.com`.
- Assurez-vous que votre politique IAM dispose de toutes les autorisations requises pour créer une instance d'accès AWS vérifié indiquée iciPolitique de création d'instances d'accès vérifié.

Étape 1 : créer une instance d'accès vérifié

Utilisez la procédure suivante pour créer une instance d'accès vérifié.

Pour créer une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation Amazon VPC, choisissez Verified Access instances, puis Create Verified Access instance.
3. (Facultatif) Dans Nom et description, entrez un nom et une description pour l'instance d'accès vérifié.
4. Pour Trust provider, conservez l'option par défaut.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
6. Choisissez Créer une instance d'accès vérifié.

Étape 2 : Configuration d'un fournisseur de confiance

Vous pouvez vous configurer en AWS IAM Identity Center tant que fournisseur de confiance.

Pour créer un fournisseur de confiance IAM Identity Center

1. Dans le volet de navigation Amazon VPC, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
2. (Facultatif) Dans le champ Nom et description, entrez le nom et la description du fournisseur de confiance Verified Access.
3. Entrez un identifiant personnalisé à utiliser ultérieurement lorsque vous utiliserez des règles de stratégie pour le nom de référence de la stratégie. Par exemple, vous pouvez entrer**`idc`**.
4. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.
5. Sous Type de fournisseur de confiance utilisateur, sélectionnez IAM Identity Center.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.
7. Choisissez Create Verified Access trust provider.

Étape 3 : associer votre fournisseur de confiance à l'instance

Utilisez la procédure suivante pour associer le fournisseur de confiance à votre instance Verified Access.

Pour associer un fournisseur de confiance à votre instance

1. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access instances.
2. Sélectionnez votre instance.
3. Choisissez Actions, puis attachez le fournisseur de confiance Verified Access.
4. Pour le fournisseur de confiance Verified Access, choisissez votre fournisseur de confiance.
5. Choisissez Attach Verified Access Trust Provider.

Étape 4 : créer un groupe d'accès vérifié

Créons un groupe que vous pourrez utiliser pour le point de terminaison que vous allez créer à l'étape suivante.

Pour créer un groupe d'accès vérifié

1. Dans le volet de navigation Amazon VPC, choisissez Verified Access groups, puis Create Verified Access group.
2. (Facultatif) Pour le tag de nom et la description, entrez un nom et une description pour le groupe.
3. Pour l'instance Verified Access, choisissez votre instance Verified Access.
4. Pour la définition de la politique, laissez ce champ vide. Vous allez créer une politique plus loin dans ce didacticiel.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.
6. Choisissez Créer un groupe d'accès vérifié.

Étape 5 : Partagez votre groupe d'accès vérifié via AWS Resource Access Manager

Au cours de cette étape, vous allez partager le groupe que vous venez de créer avec le groupe Compte AWS dans lequel s'exécute votre application cible. Pour partager un groupe à accès vérifié, vous devez l'ajouter à un partage de ressources. Si vous ne disposez pas d'un partage de ressources, vous devez d'abord en créer un.

Si vous faites partie d'une organisation et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès au groupe d'accès vérifié partagé. AWS Organizations Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès au groupe d'accès vérifié partagé après avoir accepté l'invitation.

Suivez les étapes décrites dans la section Créer un partage de ressources du Guide de l’utilisateur AWS RAM. Pour Sélectionner le type de ressource, choisissez le groupe d'accès vérifié, puis cochez la case correspondant à votre groupe d'accès vérifié.

Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur AWS RAM.

Étape 6 : Ajoutez votre application en créant un point de terminaison

Utilisez les procédures suivantes pour créer un point de terminaison. Cette étape suppose qu'une application s'exécute derrière un équilibreur de charge interne d'Elastic Load Balancing.

Pour créer un point de terminaison d'accès vérifié

1. Dans le volet de navigation Amazon VPC, choisissez Verified Access endpoints, puis Create Verified Access endpoint.
2. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
3. Pour le groupe Verified Access, choisissez votre groupe Verified Access.
4. Pour les détails de l'application, procédez comme suit :
    a. Dans le champ Domaine de l'application, entrez le nom DNS de votre application.
    b. Sous ARN du certificat de domaine, sélectionnez le nom de ressource Amazon (ARN) de votre certificat TLS public.
5. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
    a. Pour Attachment type (Type d'attachement), choisissez VPC.
    b. Pour les groupes de sécurité, sélectionnez un groupe de sécurité à associer au point de terminaison.
    c. Pour le préfixe de domaine Endpoint, entrez un identifiant personnalisé. Il sera ajouté au début du nom DNS généré par Verified Access. Pour cet exemple, nous pouvons utiliser**`my-ava-app`**.
    d. Pour le type de point de terminaison, choisissez l'équilibreur de charge.
    e. Pour Protocole, sélectionnez HTTPS ou HTTP. Cela dépend de la configuration de votre équilibreur de charge.
    f. Pour Port, saisissez le numéro de port. Cela dépend de la configuration de votre équilibreur de charge.
    g. Pour l'ARN de l'équilibreur de charge, choisissez votre équilibreur de charge.
    h. Pour les sous-réseaux, sélectionnez les sous-réseaux associés à votre équilibreur de charge.
6. Pour la définition de la stratégie, n'entrez pas de stratégie pour le moment. Nous aborderons ce sujet plus loin dans le didacticiel.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Choisissez Créer un point de terminaison d'accès vérifié.

Étape 7 : Configuration des paramètres DNS

Pour cette étape, vous devez mapper le nom de domaine de votre application (par exemple, www.myapp.example.com) au nom de domaine de votre point de terminaison Verified Access. Pour terminer le mappage DNS, créez un enregistrement de nom canonique (CNAME) auprès de votre fournisseur DNS. Après avoir créé l'enregistrement CNAME, toutes les demandes des utilisateurs adressées à votre application seront envoyées à Verified Access.

Pour obtenir le nom de domaine de votre terminal

1. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access endpoints.
2. Sélectionnez le point de terminaison que vous avez créé précédemment.
3. Choisissez l'onglet Détails du point de terminaison.
4. Copiez le domaine du point de terminaison sous le domaine du point de terminaison.

Pour ce didacticiel, le nom de domaine du point de terminaison sera`my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`.

Créez un enregistrement CNAME auprès de votre fournisseur DNS :

Nom de l'enregistrement	Type	Valeur
www.myapp.exemple.com	CNAME	my-ava-app.edge-1a 2b3c4d5e6f7g.vai-1 a2b3c4d5e6f7g.prod. verified-access.us-west-2.amazonaws. com

Étape 8 : tester la connectivité à votre application

Vous pouvez désormais tester la connectivité à votre application. Entrez le nom de domaine de votre application dans votre navigateur Web. Le comportement par défaut des politiques d'accès vérifié est de refuser toutes les demandes. Comme nous n'avons pas encore mis en place de politique permettant à quiconque d'y accéder, toutes les demandes devraient être refusées.

Étape 9 : Configuration de la politique d'accès au niveau du groupe

Utilisez la procédure suivante pour modifier le groupe d'accès vérifié et configurer une politique d'accès qui autorise la connectivité à votre application. Les détails de la politique dépendront des utilisateurs et des groupes configurés dans IAM Identity Center. Pour plus d'informations sur la création d'une politique, consultezPolitiques d'accès vérifiées.

Pour modifier un groupe d'accès vérifié

1. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access groups.
2. Sélectionnez le groupe .
3. Choisissez Actions, Modifier la politique de groupe d'accès vérifié.
4. Entrez la politique.
5. Choisissez Modifier la politique de groupe d'accès vérifié.

Étape 10 : retester la connectivité

Maintenant que votre politique de groupe est en place, vous pouvez accéder à votre application. Entrez le nom de domaine de votre application dans votre navigateur Web. La demande doit être autorisée et vous devez être redirigé vers l'application.

Nettoyage

Une fois le test terminé, suivez les étapes ci-dessous pour supprimer les ressources créées.

Pour supprimer les ressources d'accès vérifié créées avec ce didacticiel

1. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access endpoints. Sélectionnez le point de terminaison que vous souhaitez supprimer. Choisissez Actions, puis Supprimer le point de terminaison d'accès vérifié.
2. Dans le volet de navigation, sélectionnez Groupes d'accès vérifiés. Sélectionnez le groupe que vous souhaitez supprimer. Choisissez Actions, puis Supprimer le groupe d'accès vérifié. Remarque : vous devrez peut-être attendre quelques minutes jusqu'à ce que le processus de suppression du terminal soit terminé.
3. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access instances. Sélectionnez l'instance que vous avez créée pour ce didacticiel. Choisissez Actions, détachez le fournisseur

de confiance Verified Access. Sélectionnez le fournisseur de confiance dans la liste déroulante, puis choisissez Detach Verified Access Trust Provider.

4. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access trust providers. Sélectionnez le fournisseur de confiance que vous avez créé pour ce didacticiel. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
5. Dans le volet de navigation Amazon VPC, sélectionnez Verified Access instances. Sélectionnez l'instance que vous avez créée pour ce didacticiel. Choisissez Actions, puis Supprimer l'instance d'accès vérifié.

Instances d'accès vérifié

Une instance d'accès AWS vérifié est une AWS ressource qui vous aide à organiser vos fournisseurs de confiance et vos groupes d'accès vérifié.

Rubriques

Création d'une instance d'accès vérifié

Utilisez la procédure suivante pour créer une instance d'accès vérifié.

Pour créer une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Instances d'accès vérifié, puis Créer une instance d'accès vérifié.
3. (Facultatif) Dans Nom et description, entrez un nom et une description pour l'instance d'accès vérifié.
4. (Facultatif) Sélectionnez Activer les normes fédérales de traitement de l'information (FIPS) si vous avez besoin d'un accès vérifié pour être conforme à la norme FIPS.
5. (Facultatif) Pour le fournisseur de confiance, choisissez un fournisseur de confiance à associer à l'instance d'accès vérifié.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer une instance d'accès vérifié.

Associer un fournisseur de confiance à une instance

Utilisez la procédure suivante pour associer un fournisseur de confiance à une instance Verified Access.

Pour associer un fournisseur de confiance à une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, puis attachez le fournisseur de confiance Verified Access.
5. Pour le fournisseur de confiance Verified Access, choisissez un fournisseur de confiance.
6. Choisissez Attach Verified Access Trust Provider.

Détacher un fournisseur de confiance d'une instance

Utilisez la procédure suivante pour détacher un fournisseur de confiance d'une instance Verified Access.

Pour détacher un fournisseur de confiance d'une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, détachez le fournisseur de confiance Verified Access.
5. Pour le fournisseur de confiance Verified Access, choisissez le fournisseur de confiance.
6. Choisissez le fournisseur de confiance Detach Verified Access.

Supprimer une instance d'accès vérifié

Lorsque vous avez terminé d'utiliser une instance Verified Access, vous pouvez la supprimer. Avant de pouvoir supprimer une instance, vous devez supprimer tous les fournisseurs de confiance ou groupes d'accès vérifié associés.

Pour supprimer une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Choisissez Actions, puis Supprimer l'instance d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Intégration avec AWS WAF

Outre les règles d'authentification et d'autorisation appliquées par Verified Access, vous souhaiterez peut-être également appliquer une protection périmétrique. Cela peut vous aider à protéger vos applications contre des menaces supplémentaires. Vous pouvez y parvenir AWS WAF en l'intégrant à votre déploiement de Verified Access. AWS WAFest un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP (S) qui sont transmises aux ressources protégées de votre application Web. Pour plus d'informations sur les AWS WAF, consultez AWS WAF dans le Guide du développeur AWS WAF.

Vous pouvez intégrer AWS WAF Verified Access en associant une liste de contrôle d'accès AWS WAF Web (ACL) à une instance Verified Access. Une ACL Web est une AWS WAF ressource qui vous permet de contrôler avec précision toutes les requêtes Web HTTP (S) auxquelles répond votre ressource protégée. Pendant le traitement de la demande d'AWS WAFassociation ou de dissociation, le statut de tous les points de terminaison Verified Access attachés à l'instance est affiché sous la forme. `updating` Une fois la demande terminée, le statut revient à`active`. Vous pouvez consulter le statut dans le AWS Management Console ou en décrivant le point de terminaison à l'aide duAWS CLI.

> **Note**
>
> Vous pouvez également utiliser la AWS WAF console ou l'API pour réaliser cette intégration. Vous aurez besoin du nom de ressource Amazon (ARN) de votre instance Verified Access. Vous pouvez créer cet ARN en utilisant le format suivant : `arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`

Rubriques

Autorisations IAM requises pour l'intégration AWS WAF

L'intégration à Verified Access inclut des actions AWS WAF avec autorisation uniquement qui ne correspondent pas directement à une opération d'API. Ces actions sont indiquées dans la référence d'autorisation de AWS Identity and Access Management service avec`[permission only]`. Consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans la référence d'autorisation de service.

Pour utiliser une ACL Web, votre AWS Identity and Access Management principal doit disposer des autorisations suivantes.

- `ec2:AssociateVerifiedAccessInstanceWebAcl`
- `ec2:DisassociateVerifiedAccessInstanceWebAcl`
- `ec2:DescribeVerifiedAccessInstanceWebAclAssociations`
- `ec2:GetVerifiedAccessInstanceWebAcl`

Associer une ACL AWS WAF Web

Les étapes suivantes montrent comment associer une liste de contrôle d'accès AWS WAF Web (ACL) à une instance d'accès vérifié à l'aide duAWS Management Console.

> **Tip**
>
> Vous devez disposer d'une ACL AWS WAF Web existante pour effectuer la procédure ci-dessous. Pour plus d'informations sur les ACL Web, consultez les listes de contrôle d'accès Web dans le Guide du AWS WAF développeur.

Pour associer une ACL AWS WAF Web à une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.
5. Choisissez Actions, puis Associer une ACL Web.
6. Pour l'ACL Web, choisissez une ACL Web existante, puis choisissez Associate Web ACL.

Vous pouvez également utiliser le AWS Management Console for AWS WAF pour accomplir cette tâche. Pour plus d'informations, consultez la section Associer ou dissocier une ACL Web à une ressource AWS dans le manuel du AWS WAF développeur.

Vérifier l'état de l'AWS WAFintégration

Vous pouvez vérifier si une liste de contrôle d'accès AWS WAF Web (ACL) est associée ou non à une instance d'accès vérifié en utilisant leAWS Management Console.

Pour consulter l'état de l'AWS WAFintégration avec une instance Verified Access

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.
5. Vérifiez les informations répertoriées sous État de l'intégration WAF. Le statut sera affiché comme Associé ou Non associé, ainsi que l'identifiant ACL Web, s'il est dans l'état Associé.

Dissocier une ACL AWS WAF Web

Les étapes suivantes montrent comment dissocier une liste de contrôle d'accès AWS WAF Web (ACL) d'une instance d'accès vérifié à l'aide duAWS Management Console.

Pour dissocier une ACL AWS WAF Web d'une instance d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.

5. Choisissez Actions, puis Dissocier l'ACL Web.
6. Confirmez en choisissant Dissociate Web ACL.

Vous pouvez également utiliser le AWS Management Console for AWS WAF pour accomplir cette tâche. Pour plus d'informations, consultez la section Associer ou dissocier une ACL Web à une ressource AWS dans le manuel du AWS WAF développeur.

Conformité à la norme FIPS pour l'accès vérifié

La norme fédérale de traitement de l'information (FIPS) est une norme gouvernementale américaine et canadienne qui spécifie les exigences de sécurité pour les modules cryptographiques qui protègent les informations sensibles. Accès vérifié par AWSoffre la possibilité de configurer votre environnement pour qu'il adhère à la publication FIPS 140-2. La conformité à la norme FIPS pour l'accès vérifié est disponible dans les AWS régions suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Canada (Centre)

Cette page explique comment configurer un environnement d'accès vérifié, nouveau ou existant, pour qu'il soit conforme à la norme FIPS.

Rubriques

Configuration d'un environnement d'accès vérifié existant pour la conformité à la norme FIPS

Si vous disposez d'un environnement d'accès vérifié existant et que vous souhaitez le configurer pour qu'il soit conforme à la norme FIPS, certaines ressources devront être supprimées et recréées afin d'activer la conformité FIPS.

Pour reconfigurer un Accès vérifié par AWS environnement existant afin qu'il soit conforme à la norme FIPS, suivez les étapes ci-dessous.

1. Supprimez vos points de terminaison, groupes et instance Verified Access d'origine. Vos fournisseurs de confiance configurés peuvent être réutilisés.
2. Créez une instance d'accès vérifié, en veillant à activer les normes fédérales de traitement de l'information (FIPS) lors de la création. Lors de la création, associez également le fournisseur de confiance Verified Access que vous souhaitez utiliser en le sélectionnant dans la liste déroulante.
3. Créez un groupe d'accès vérifié. Lors de la création du groupe, vous l'associez à l'instance Verified Access qui vient d'être créée.
4. Créez-en un ou plusieursPoints de terminaison d'accès vérifiés. Lors de la création de vos points de terminaison, vous les associez au groupe créé à l'étape précédente.

Configuration d'un nouvel environnement d'accès vérifié pour la conformité à la norme FIPS

Pour configurer un nouvel Accès vérifié par AWS environnement conforme à la norme FIPS, suivez les étapes ci-dessous.

1. Configurez un fournisseur de confiance. Vous devrez créer un fournisseur de confiance en matière d'identité utilisateur et (éventuellement) un fournisseur de confiance basé sur l'appareil, en fonction de vos besoins.
2. Créez une instance d'accès vérifié, en veillant à activer les normes fédérales de traitement de l'information (FIPS) pendant le processus. Lors de la création, attachez également le fournisseur de confiance Verified Access que vous avez créé à l'étape précédente, en le sélectionnant dans la liste déroulante.
3. Créez un groupe d'accès vérifié. Lors de la création du groupe, vous l'associez à l'instance Verified Access qui vient d'être créée.
4. Créez-en un ou plusieursPoints de terminaison d'accès vérifiés. Lors de la création de vos points de terminaison, vous les associez au groupe créé à l'étape précédente.

Faites confiance aux fournisseurs pour un accès vérifié

Un fournisseur de confiance est un service qui envoie des informations sur les utilisateurs et les appareils à AWS Verified Access. Ces informations sont appelées contexte de confiance. Il peut inclure des attributs basés sur l'identité de l'utilisateur, tels qu'une adresse e-mail ou l'adhésion à l'organisation « commerciale », ou des informations sur l'appareil telles que les correctifs de sécurité installés ou la version du logiciel antivirus.

Verified Access prend en charge les catégories de fournisseurs de confiance suivantes :

- Identité utilisateur : service de fournisseur d'identité (IdP) qui stocke et gère les identités numériques des utilisateurs.
- Gestion des appareils : système de gestion des appareils pour les appareils tels que les ordinateurs portables, les tablettes et les smartphones.

Table des matières

Fournisseurs de confiance en matière d'identité utilisateur

Vous pouvez choisir d'utiliser l'un AWS IAM Identity Center ou l'autre fournisseur de confiance en matière d'identité utilisateur compatible avec OpenID Connect.

Table des matières

Utiliser IAM Identity Center en tant que fournisseur de confiance

Vous pouvez l'utiliser AWS IAM Identity Center comme fournisseur de confiance en matière d'identité utilisateur avec AWS Verified Access.

Prérequis et considérations

- Votre instance IAM Identity Center doit être une AWS Organizations instance. Une instance IAM Identity Center d'un AWS compte autonome ne fonctionnera pas.
- Votre instance IAM Identity Center doit être activée dans la même AWS région que celle dans laquelle vous souhaitez créer le fournisseur de confiance Verified Access.

Voir Gérer les instances d'organisation et de compte d'IAM Identity Center dans le guide de l'AWS IAM Identity Centerutilisateur pour plus de détails sur les différents types d'instances.

Création d'un fournisseur de confiance IAM Identity Center

Une fois IAM Identity Center activé sur votre AWS compte, vous pouvez utiliser la procédure suivante pour configurer IAM Identity Center en tant que fournisseur de confiance pour l'accès vérifié.

Pour créer un fournisseur de confiance IAM Identity Center (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.
4. Pour le nom de référence de la stratégie, entrez un identifiant à utiliser ultérieurement lors de l'utilisation des règles de stratégie.
5. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.
6. Sous Type de fournisseur de confiance utilisateur, sélectionnez IAM Identity Center.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Choisissez Create Verified Access trust provider.

Pour créer un fournisseur de confiance (AWSCLI) IAM Identity Center

- create-verified-access-trust-fournisseur () AWS CLI

Supprimer un fournisseur de confiance IAM Identity Center

Avant de pouvoir supprimer un fournisseur de confiance, vous devez supprimer toutes les configurations de point de terminaison et de groupe de l'instance à laquelle le fournisseur de confiance est attaché.

Pour supprimer un fournisseur de confiance IAM Identity Center (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Verified Access trust providers.
3. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
4. Confirmez la suppression en entrant `delete` dans la zone de texte.
5. Sélectionnez Delete (Supprimer).

Pour supprimer un fournisseur de confiance (AWSCLI) IAM Identity Center

- delete-verified-access-trust-fournisseur () AWS CLI

Utilisation d'un fournisseur de confiance OpenID Connect

AWSVerified Access prend en charge les fournisseurs d'identité qui utilisent les méthodes standard OpenID Connect (OIDC). Vous pouvez utiliser des fournisseurs compatibles OIDC en tant que fournisseurs de confiance en matière d'identité utilisateur avec accès vérifié. Cependant, en raison du large éventail de fournisseurs OIDC potentiels, AWS il n'est pas en mesure de tester chaque intégration OIDC avec Verified Access.

Verified Access obtient les données de confiance qu'il évalue auprès du fournisseur OIDC. `UserInfo Endpoint` Le `Scope` paramètre est utilisé pour déterminer quels ensembles de données de confiance seront récupérés. Une fois les données de confiance reçues, la politique d'accès vérifié est évaluée par rapport à celles-ci.

> **Note**
>
> Verified Access n'utilise pas les données de confiance `ID token` envoyées par le fournisseur OIDC lors de l'évaluation de la politique d'accès vérifié. Seules les données de confiance provenant de `UserInfo Endpoint` sont évaluées par rapport à la politique.

Table des matières

Conditions préalables à la création d'un fournisseur de confiance OIDC

Vous devrez recueillir les informations suivantes directement auprès du service de votre fournisseur de confiance :

- Emetteur
- Point final d'autorisation
- Point de terminaison de jeton
- UserInfo point final
- ID de client
- Secret client
- Portée

Création d'un fournisseur de confiance OIDC

Utilisez la procédure suivante pour créer un OIDC en tant que fournisseur de confiance.

Pour créer un fournisseur de confiance OIDC (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.
4. Pour le nom de référence de la stratégie, entrez un identifiant à utiliser ultérieurement lors de l'utilisation des règles de stratégie.
5. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.

6. Sous Type de fournisseur de confiance utilisateur, sélectionnez OIDC (OpenID Connect).
7. Dans Émetteur, entrez l'identifiant de l'émetteur OIDC.
8. Pour Point de terminaison d'autorisation, entrez l'URL complète du point de terminaison d'autorisation.
9. Pour le point de terminaison du jeton, entrez l'URL complète du point de terminaison du jeton.
10. Pour Point de terminaison utilisateur, entrez l'URL complète du point de terminaison utilisateur.
11. Entrez l'identifiant du client OAuth 2.0 pour l'ID client.
12. Entrez le secret du client OAuth 2.0 pour le secret du client.
13. Entrez une liste délimitée par des espaces de champs définis avec votre fournisseur d'identité. Au minimum, la portée « openid » est requise pour Scope.
14. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
15. Choisissez Create Verified Access trust provider.

> **Note**
>
> Vous devrez ajouter un URI de redirection à la liste d'autorisation de votre fournisseur OIDC. Vous souhaiterez utiliser le point `ApplicationDomain` de terminaison Verified Access à cette fin. Vous pouvez le trouver dans l'AWS Management Consoleonglet Détails de votre point de terminaison d'accès vérifié ou en utilisant le AWS CLI pour décrire le point de terminaison. Ajoutez ce qui suit à la liste des autorisations de votre fournisseur OIDC : https :///oauth2/idpresponse `ApplicationDomain`

Pour créer un fournisseur de confiance OIDC (AWSCLI)

- create-verified-access-trust-fournisseur () AWS CLI

Modifier un fournisseur de confiance OIDC

Après avoir créé un fournisseur de confiance, vous pouvez mettre à jour sa configuration.

Pour modifier un fournisseur de confiance OIDC (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Fournisseurs de confiance Verified Access, puis sélectionnez le fournisseur de confiance que vous souhaitez modifier sous Fournisseurs de confiance Verified Access.
3. Choisissez Actions, puis Modifier le fournisseur de confiance Verified Access.
4. Modifiez les options que vous souhaitez modifier.
5. Choisissez Modifier le fournisseur de confiance Verified Access.

Pour modifier un fournisseur de confiance OIDC (AWSCLI)

- modify-verified-access-trust-fournisseur () AWS CLI

Supprimer un fournisseur de confiance OIDC

Avant de supprimer un fournisseur de confiance utilisateur, vous devez d'abord supprimer toutes les configurations de point de terminaison et de groupe de l'instance à laquelle le fournisseur de confiance est attaché.

Pour supprimer un fournisseur de confiance OIDC (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Verified Access trust providers.
3. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
4. Confirmez la suppression en entrant `delete` dans la zone de texte.
5. Sélectionnez Delete (Supprimer).

Pour supprimer un fournisseur de confiance OIDC (AWSCLI)

- delete-verified-access-trust-fournisseur () AWS CLI

Fournisseurs de confiance basés sur des appareils

Vous pouvez utiliser des fournisseurs de confiance en matière d'appareils dotés d'AWSun accès vérifié. Vous pouvez utiliser un ou plusieurs fournisseurs de confiance pour appareils avec votre instance Verified Access.

Table des matières

Fournisseurs de confiance en matière d'appareils compatibles

Les fournisseurs de confiance en matière d'appareils suivants peuvent être intégrés à Verified Access :

- CrowdStrike — Sécurisation des applications privées avec CrowdStrike accès vérifié
- Jamf — Intégration de l'accès vérifié à l'identité des appareils Jamf
- JumpCloud — Intégration JumpCloud et accès AWS vérifié

Création d'un fournisseur de confiance basé sur l'appareil

Suivez ces étapes pour créer et configurer un fournisseur de confiance pour les appareils à utiliser avec Verified Access.

Pour créer un fournisseur de confiance pour les appareils à accès vérifié (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.
4. Entrez un identifiant à utiliser ultérieurement lorsque vous utiliserez des règles de stratégie pour le nom de référence de la stratégie.
5. Pour le type de fournisseur de confiance, sélectionnez Identité de l'appareil.
6. Pour le type d'identité de l'appareil CrowdStrike, choisissez Jamf ou JumpCloud.
7. Dans le champ ID du locataire, entrez l'identifiant de l'application du locataire.

8. (Facultatif) Pour l'URL de la clé de signature publique, entrez l'URL de la clé unique partagée par le fournisseur de confiance de votre appareil. (Ce paramètre n'est pas obligatoire pour Jamf CrowdStrike ou Jumpcloud.)
9. Choisissez Create Verified Access trust provider.

> **Note**
>
> Vous devrez ajouter un URI de redirection à la liste d'autorisation de votre fournisseur OIDC. Vous souhaiterez utiliser le point `DeviceValidationDomain` de terminaison Verified Access à cette fin. Vous pouvez le trouver dans l'AWS Management Consoleonglet Détails de votre point de terminaison d'accès vérifié ou en utilisant le AWS CLI pour décrire le point de terminaison. Ajoutez ce qui suit à la liste des autorisations de votre fournisseur OIDC : https :///oauth2/idpresponse `DeviceValidationDomain`

Pour créer un fournisseur de confiance pour les appareils à accès vérifié (AWSCLI)

- create-verified-access-trust-fournisseur () AWS CLI

Modifier un fournisseur de confiance basé sur un appareil

Après avoir créé un fournisseur de confiance, vous pouvez mettre à jour sa configuration.

Pour modifier un fournisseur de confiance pour les appareils à accès vérifié (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access trust providers.
3. Sélectionnez le fournisseur de confiance.
4. Choisissez Actions, puis sélectionnez Modifier le fournisseur de confiance Verified Access.
5. Modifiez la description selon vos besoins.
6. (Facultatif) Pour l'URL de la clé de signature publique, modifiez l'URL de la clé unique partagée par le fournisseur de confiance de votre appareil. (Ce paramètre n'est pas obligatoire si le fournisseur de confiance de votre appareil est Jamf CrowdStrike ou Jumpcloud.)
7. Choisissez Modifier le fournisseur de confiance Verified Access.

Pour modifier un fournisseur de confiance (AWSCLI) de périphériques à accès vérifié

- modify-verified-access-trust-fournisseur () AWS CLI

Supprimer un fournisseur de confiance basé sur un appareil

Lorsque vous en avez terminé avec un fournisseur de confiance, vous pouvez le supprimer.

Pour supprimer un fournisseur de confiance d'appareils à accès vérifié (AWSconsole)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access trust providers.
3. Sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Fournisseurs de confiance à accès vérifié.
4. Choisissez Actions, puis sélectionnez Supprimer le fournisseur de confiance Verified Access.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer un fournisseur de confiance (AWSCLI) à accès vérifié

- delete-verified-access-trust-fournisseur () AWS CLI

Groupes d'accès vérifiés

Un groupe d'accès AWS vérifié est un ensemble de points de terminaison Verified Access et une politique d'accès vérifié au niveau du groupe. Chaque point de terminaison d'un groupe partage la politique d'accès vérifié. Vous pouvez utiliser des groupes pour rassembler les terminaux qui ont des exigences de sécurité communes. Cela peut contribuer à simplifier l'administration des politiques en utilisant une seule politique pour répondre aux besoins de sécurité de plusieurs applications.

Par exemple, vous pouvez regrouper toutes les applications de vente et définir une politique d'accès à l'échelle du groupe. Vous pouvez ensuite utiliser cette politique pour définir un ensemble commun d'exigences de sécurité minimales pour toutes les applications de vente. Cette approche permet de simplifier l'administration des politiques.

Lorsque vous créez un groupe VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccess Au cours du processus de création d'un point de terminaison, vous allez associer le point de terminaison à un groupe.

Tâches

- créer un groupe VAccès VAccès VAccès VAccès
- Modifier une stratégie VAccès VAccès VAccès VAccès VAccès
- supprimer un groupe VAccès VAccès VAccès VAccès

créer un groupe VAccès VAccès VAccès VAccès

Utilisez la procédure suivante pour créer un groupe VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès V

créer un groupe VAccès VAccès VAccès VAccès VAccès

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes d'accès vérifiés, puis Créer un groupe d'accès vérifié.
3. (Facultatif) Dans les champs Nom et Description, entrez le nom et la description du groupe.
4. Pour l'instance Verified Access, sélectionnez une instance Verified Access à associer au groupe.
5. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié à appliquer au groupe.

6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer un groupe d'accès vérifié.

Modifier une stratégie VAccès VAccès VAccès VAccès VAccès

Utilisez la procédure suivante pour modifier une stratégie de groupe VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccess.

Pour modifier une stratégie VAccès VAccès VAccès VAccès VAccess Access

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès V
3. Choisissez Actions, puis Modifier la politique de groupe Verified Access.
4. (Facultatif) Activez une stratégie de cycle de vie.
5. (Facultatif) Pour Politique, entrez une politique d'accès vérifié à appliquer au groupe.
6. Choisissez Modifier la politique du groupe Verified Access.

supprimer un groupe VAccès VAccès VAccès VAccès

Lorsque vous avez VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccès VAccess

supprimer un groupe VAccès VAccès VAccès VAccès VAccès

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes VAccès VAccès VAccès VAccès VAccès VAccès V
3. Sélectionnez le groupe .
4. Choisissez Actions, puis Supprimer le groupe d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Points de terminaison d'accès vérifiés

Un point de terminaison d'accès vérifié représente une application. Chaque point de terminaison est associé à un groupe d'accès vérifié et hérite de la politique d'accès du groupe. Vous pouvez éventuellement associer une politique de point de terminaison spécifique à l'application à chaque point de terminaison.

Table des matières

Types de points de terminaison d'accès vérifiés

Les types de terminaux possibles sont les suivants :

- Équilibreur de charge : les demandes d'application sont envoyées à un équilibreur de charge pour être distribuées à votre application.
- Interface réseau : les demandes d'application sont envoyées à une interface réseau à l'aide du protocole et du port spécifiés.

VPC et sous-réseaux partagés

Les comportements relatifs aux sous-réseaux VPC partagés sont les suivants :

- Les points de terminaison Verified Access sont pris en charge par le partage de sous-réseaux VPC. Un participant peut créer un point de terminaison d'accès vérifié dans un sous-réseau partagé.

- Le participant qui a créé le point de terminaison sera le propriétaire du point de terminaison et la seule personne autorisée à modifier le point de terminaison. Le propriétaire du VPC ne sera pas autorisé à modifier le point de terminaison.
- Les points de terminaison Verified Access ne peuvent pas être créés dans une zone AWS locale et le partage via les zones locales n'est donc pas possible.

Pour plus d'informations, consultez Partager votre VPC avec d'autres comptes dans le Guide de l'utilisateur Amazon VPC.

Création d'un point de terminaison d'équilibrage de charge pour Verified Access

Utilisez la procédure suivante pour créer un point de terminaison d'équilibreur de charge. Pour plus d'informations sur les équilibreurs de charge, consultez le guide de l'utilisateur d'Elastic Load Balancing.

Prérequis

- Seul le trafic IPv4 est pris en charge.
- Seuls les protocoles HTTP et HTTPS sont pris en charge.
- L'équilibreur de charge doit être soit un Application Load Balancer, soit un Network Load Balancer, et il doit s'agir d'un équilibreur de charge interne.
- L'équilibreur de charge et les sous-réseaux doivent appartenir au même cloud privé virtuel (VPC).
- Les équilibreurs de charge HTTPS peuvent utiliser des certificats TLS autosignés ou publics.
- Vous devez fournir un nom de domaine pour votre application. Il s'agit du nom DNS public que vos utilisateurs utiliseront pour accéder à votre application. Vous devrez également fournir un certificat SSL public avec un CN correspondant à ce nom de domaine. Vous pouvez créer ou importer le certificat à l'aide deAWS Certificate Manager.

Pour créer un point de terminaison d'équilibrage de charge

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez Créer un point de terminaison d'accès vérifié.

4. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
5. Pour le groupe d'accès vérifié, choisissez un groupe d'accès vérifié pour le point de terminaison.
6. Pour les détails de l'application, procédez comme suit :
   a. Dans le champ Domaine de l'application, entrez le nom DNS de votre application.
   b. Dans le champ ARN du certificat de domaine, choisissez le certificat TLS public.
7. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
   a. Pour Attachment type (Type d'attachement), choisissez VPC.
   b. Pour les groupes de sécurité, choisissez les groupes de sécurité pour le point de terminaison. Le trafic provenant du point de terminaison Verified Access qui entre dans votre équilibreur de charge sera associé à ce groupe de sécurité.
   c. Pour le préfixe de domaine du point de terminaison, entrez un identifiant personnalisé à ajouter au nom DNS généré par Verified Access pour le point de terminaison.
   d. Pour le type de point de terminaison, choisissez l'équilibreur de charge.
   e. Dans le champ Protocole, choisissez HTTPS ou HTTP.
   f. Sous Port, entrez le numéro de port.
   g. Pour l'ARN de l'équilibreur de charge, choisissez l'équilibreur de charge.
   h. Pour les sous-réseaux, choisissez les sous-réseaux pour votre équilibreur de charge.
8. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié pour le point de terminaison.
9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison d'accès vérifié.

Création d'un point de terminaison d'interface réseau pour Verified Access

Utilisez la procédure suivante pour créer un point de terminaison d'interface réseau.

Prérequis

- Seul le trafic IPv4 est pris en charge.

- Seuls les protocoles HTTP et HTTPS sont pris en charge.
- L'interface réseau doit appartenir au même cloud privé virtuel (VPC) que les groupes de sécurité.
- Nous utilisons l'adresse IP privée sur l'interface réseau pour transférer le trafic.
- Vous devez fournir un nom de domaine pour votre application. Il s'agit du nom DNS public que vos utilisateurs utiliseront pour accéder à votre application. Vous devrez également fournir un certificat SSL public avec un CN correspondant à ce nom de domaine. Vous pouvez créer ou importer le certificat à l'aide deAWS Certificate Manager.

Pour créer un point de terminaison d'interface réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez Créer un point de terminaison d'accès vérifié.
4. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
5. Pour le groupe d'accès vérifié, choisissez un groupe d'accès vérifié pour le point de terminaison.
6. Pour les détails de l'application, procédez comme suit :
   a. Dans le champ Domaine de l'application, entrez le nom DNS de votre application.
   b. Dans le champ ARN du certificat de domaine, choisissez le certificat TLS public.
7. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
   a. Pour Attachment type (Type d'attachement), choisissez VPC.
   b. Pour les groupes de sécurité, choisissez les groupes de sécurité pour le point de terminaison. Le trafic provenant du point de terminaison d'accès vérifié qui entre dans votre interface réseau sera associé à ce groupe de sécurité.
   c. Pour le préfixe de domaine du point de terminaison, entrez un identifiant personnalisé à ajouter au nom DNS généré par Verified Access pour le point de terminaison.
   d. Pour le type de point de terminaison, choisissez Interface réseau.
   e. Dans le champ Protocole, choisissez HTTPS ou HTTP.
   f. Sous Port, entrez le numéro de port.
   g. Pour Interface réseau, choisissez l'interface réseau.
8. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié pour le point de terminaison.

9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison d'accès vérifié.

Autoriser le trafic provenant de votre point de terminaison Verified Access

Vous pouvez configurer les groupes de sécurité pour vos applications afin qu'ils autorisent le trafic provenant de votre point de terminaison Verified Access. Pour ce faire, ajoutez une règle entrante qui indique le groupe de sécurité du point de terminaison comme source. Nous vous recommandons de supprimer toutes les règles entrantes supplémentaires afin que votre application ne reçoive du trafic que depuis votre point de terminaison Verified Access.

Nous vous recommandons de conserver vos règles sortantes existantes.

Pour mettre à jour les règles du groupe de sécurité pour votre application

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez le point de terminaison d'accès vérifié, recherchez les ID du groupe de sécurité dans l'onglet Détails et copiez l'ID du groupe de sécurité pour votre point de terminaison.
4. Dans le panneau de navigation, choisissez Groupes de sécurité.
5. Cochez la case correspondant au groupe de sécurité associé à votre cible, puis choisissez Actions, Modifier les règles entrantes.
6. Pour ajouter une règle de groupe de sécurité autorisant le trafic provenant de votre point de terminaison Verified Access, procédez comme suit :
    a. Choisissez Ajouter une règle.
    b. Dans Type, choisissez Tout le trafic ou le trafic spécifique à autoriser.
    c. Pour Source, choisissez Personnalisé et collez l'ID du groupe de sécurité de votre terminal.
7. (Facultatif) Pour exiger que le trafic provienne uniquement de votre point de terminaison Verified Access, supprimez toutes les autres règles du groupe de sécurité entrant.
8. Sélectionnez Enregistrer les règles.

Modifier un point de terminaison d'accès vérifié

Après avoir créé un point de terminaison d'accès vérifié, vous pouvez mettre à jour sa configuration.

Pour modifier un point de terminaison d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, Modifier le point de terminaison d'accès vérifié.
5. Modifiez les détails du point de terminaison selon vos besoins.
6. Choisissez Modifier le point de terminaison d'accès vérifié.

Modifier une politique de point de terminaison d'accès vérifié

Après avoir créé un point de terminaison d'accès vérifié, vous pouvez modifier sa politique.

Pour modifier une politique de point de terminaison d'accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison dont vous souhaitez modifier la politique.
4. Choisissez Actions, puis Modifier la politique du point de terminaison d'accès vérifié.
5. (Facultatif) Activez ou désactivez la politique d'activation en fonction de votre objectif actuel.
6. (Facultatif) Pour Politique, entrez une politique d'accès vérifié à appliquer au point de terminaison.
7. Choisissez Modifier la politique du point de terminaison d'accès vérifié.

Supprimer un point de terminaison d'accès vérifié

Lorsque vous avez terminé d'utiliser un point de terminaison Verified Access, vous pouvez le supprimer.

Pour supprimer un point de terminaison avec accès vérifié

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, puis Supprimer le point de terminaison d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Données de confiance provenant de fournisseurs de confiance

Les données de confiance sont des données envoyées à AWS Verified Access par un fournisseur de confiance. Il est également parfois appelé « réclamations des utilisateurs » ou « contexte de confiance ». Les données incluent généralement des informations concernant un utilisateur ou un appareil. Les exemples de données de confiance incluent le courrier électronique de l'utilisateur, l'appartenance à un groupe, la version du système d'exploitation de l'appareil, l'état de sécurité de l'appareil, etc. Les informations envoyées varient en fonction du fournisseur de confiance. Vous devez donc vous référer à la documentation de votre fournisseur de confiance pour obtenir une liste complète et actualisée des données de confiance.

Toutefois, en utilisant les fonctionnalités de journalisation des accès vérifiés, vous pouvez également voir quelles données de confiance sont envoyées par votre fournisseur de confiance. Cela peut être très utile lorsque vous définissez des politiques qui autorisent ou refusent l'accès à vos applications. Pour plus d'informations sur l'inclusion d'un contexte de confiance dans vos journaux, consultezY compris le contexte de confiance.

Cette section contient des exemples de données de confiance et des exemples pour commencer à rédiger des politiques. Les informations fournies ici sont uniquement destinées à des fins d'illustration et ne constituent pas une référence officielle.

Table des matières

Contexte par défaut de Verified Access

AWSVerified Access inclut par défaut certains éléments relatifs à la requête HTTP en cours dans toutes les évaluations de Cedar, quels que soient vos fournisseurs de confiance configurés. Lorsqu'une politique est évaluée, Verified Access inclut des données relatives à la requête HTTP en cours dans le contexte Cedar sous le`context.http_request key`. Vous pouvez rédiger une

politique qui évalue par rapport aux données si vous le souhaitez. Le schéma JSON suivant indique quelles données sont incluses dans l'évaluation.

```
{
     "title": "HTTP Request data included by Verified Access",
     "type": "object",
     "properties": {
         "user_agent": {
             "type": "string",
             "description": "The value of the User-Agent request header"
         },
         "x_forwarded_for": {
             "type": "string",
             "description": "The value of the X-Forwarded-For request header"
         },
         "http_method": {
             "type": "string",
             "description": "The HTTP Method provided (e.g. GET or POST)"
         },
         "hostname": {
             "type": "string",
             "description": "The value of the Host request header"
         },
         "port": {
            "type": "integer",
            "description": "The value of the verified access endpoint port"
         },
         "client_ip": {
             "type": "string",
             "description": "User ip connecting to the verified access endpoint"
         }
     }
 }
```

Voici un exemple de politique qui évalue par rapport aux données de requête HTTP.

```
forbid(principal, action, resource) when {
   context.http_request.http_method == "POST"
   && !(context.identity.roles.contains("Administrator"))
 };
```

AWS IAM Identity Center

Lorsqu'une politique est évaluée, si vous la définissez en AWS IAM Identity Center tant que fournisseur de confiance, AWS Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez.

> **Note**
>
> La clé de contexte de votre fournisseur de confiance provient du nom de référence de politique que vous configurez lorsque vous créez le fournisseur de confiance. Par exemple, si vous configurez le nom de référence de la politique comme « idp123 », la clé de contexte sera « context.idp123 ». Vérifiez que vous utilisez la bonne clé de contexte lorsque vous créez la politique.

Le schéma JSON suivant indique quelles données sont incluses dans l'évaluation.

```
{
   "title": "AWS IAM Identity Center context specification",
   "type": "object",
   "properties": {
     "user": {
       "type": "object",
       "properties": {
         "user_id": {
           "type": "string",
           "description": "a unique user id generated by AWS IdC"
         },
         "user_name": {
           "type": "string",
           "description": "username provided in the directory"
         },
         "email": {
           "type": "object",
           "properties": {
             "address": {
               "type": "email",
               "description": "email address associated with the user"
             },
```

```
              "verified": {
                "type": "boolean",
                "description": "whether the email address has been verified by AWS IdC"
              }
            }
          }
        }
      },
      "groups": {
        "type": "object",
        "description": "A list of groups the user is a member of",
        "patternProperties": {
          "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{12}$": {
            "type": "object",
            "description": "The Group ID of the group",
            "properties": {
              "group_name": {
                "type": "string",
                "description": "The customer-provided name of the group"
              }
            }
          }
        }
      }
    }
  }
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par AWS IAM Identity Center.

```
permit(principal, action, resource) when {
   context.idc.user.email.verified == true
   // User is in the "sales" group with specific ID
   && context.idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
 };
```

> **Note**
>
> Comme les noms de groupes peuvent être modifiés, IAM Identity Center fait référence aux groupes en utilisant leur identifiant de groupe. Cela permet d'éviter de violer une déclaration de politique lorsque vous modifiez le nom d'un groupe.

Prestataires de confiance tiers

Cette section décrit les données de confiance fournies à AWS Verified Access par des fournisseurs de confiance tiers.

> **Note**
>
> La clé de contexte de votre fournisseur de confiance provient du nom de référence de politique que vous configurez lorsque vous créez le fournisseur de confiance. Par exemple, si vous configurez le nom de référence de la politique comme « idp123 », la clé de contexte sera « context.idp123 ». Assurez-vous d'utiliser la bonne clé de contexte lorsque vous créez la politique.

Table des matières

Extension de navigateur

Si vous envisagez d'intégrer un contexte de confiance aux appareils dans vos politiques d'accès, vous aurez besoin de l'extension de navigateur AWS Verified Access ou de l'extension de navigateur d'un autre partenaire. Verified Access est actuellement compatible avec les navigateurs Google Chrome et Mozilla Firefox.

Nous soutenons actuellement trois fournisseurs de confiance en matière d'appareils : Jamf (qui prend en charge les appareils macOS), CrowdStrike (qui prend en charge les appareils Windows 11 et Windows 10) et JumpCloud (qui prend en charge à la fois Windows et macOS).

- Si vous utilisez les données de confiance Jamf dans vos politiques, vos utilisateurs doivent télécharger et installer l'extension de navigateur AWS Verified Access depuis le Chrome Web Store ou le site du module complémentaire Firefox sur leurs appareils.
- Si vous utilisez des données de CrowdStrikeconfiance dans vos politiques, vos utilisateurs doivent d'abord installer le AWSVerified Access Native Messaging Host (lien de téléchargement direct). Ce composant est nécessaire pour obtenir les données de confiance de l' CrowdStrike agent exécuté sur les appareils des utilisateurs. Ensuite, après avoir installé ce composant, les utilisateurs doivent installer l'extension de navigateur AWS Verified Access depuis le Chrome Web Store ou le site du module complémentaire Firefox sur leurs appareils.
- Si vous l'utilisez JumpCloud, l'extension de JumpCloud navigateur du Chrome Web Store ou du site du module complémentaire Firefox doit être installée sur leurs appareils.

Jamf

Jamf est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous définissez Jamf comme un fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le schéma JSON suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation de Jamf avec accès AWS vérifié, consultez la section Intégration d'AWS Verified Access à Jamf Device Identity sur le site Web de Jamf.

```
{
    "title": "Jamf device data specification",
    "type": "object",
    "properties": {
        "iss": {
            "type": "string",
            "description": "\"Issuer\" - the Jamf customer ID"
        },
        "iat": {
            "type": "integer",
            "description": "\"Issued at Time\" - a unixtime (seconds since epoch) value
 of when the device information data was generated"
        },
        "exp": {
            "type": "integer",
```

```
            "description": "\"Expiration\" - a unixtime (seconds since epoch) value for
 when this device information is no longer valid"
        },
        "sub": {
            "type": "string",
            "description": "\"Subject\" - either the hardware UID or a value generated
 based on device location"
        },
        "groups": {
            "type": "array",
            "description": "Group IDs from UEM connector sync",
            "items": {
                "type": "string"
            }
        },
        "risk": {
            "type": "string",
            "enum": [
                "HIGH",
                "MEDIUM",
                "LOW",
                "SECURE",
                "NOT_APPLICABLE"
            ],
            "description": "a Jamf-reported level of risk associated with the device."
        },
        "osv": {
            "type": "string",
            "description": "The version of the OS that is currently running, in Apple
 version number format (https://support.apple.com/en-us/HT201260)"
        }
    }
}
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par Jamf.

```
permit(principal, action, resource) when {
   context.jamf.risk == "LOW"
};
```

Cedar fournit une `.contains()` fonction utile pour vous aider avec des énumérations telles que le score de risque de Jamf.

```
permit(principal, action, resource) when {
   ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

CrowdStrike

CrowdStrike est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous la définissez en CrowdStrike tant que fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le schéma JSON suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation CrowdStrike avec AWS Verified Access, voir Sécurisation des applications privées avec Verified Access CrowdStrike et AWS Verified Access sur le GitHub site Web.

```
{
  "title": "CrowdStrike device data specification",
  "type": "object",
  "properties": {
    "assessment": {
      "type": "object",
      "description": "Data about CrowdStrike's assessment of the device",
      "properties": {
        "overall": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts as a weighted
 average of the OS and and Sensor Config scores"
        },
        "os": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the OS-
specific settings monitored on the host"
        },
        "sensor_config": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the
 different sensor policies monitored on the host"
        },
        "version": {
```

```
          "type": "string",
          "description": "The version of the scoring algorithm being used"
        }
      }
    },
    "cid": {
      "type": "string",
      "description": "Customer ID (CID) unique to the customer's environemnt"
    },
    "exp": {
      "type": "integer",
      "description": "unixtime, The expiration time of the token"
    },
    "iat": {
      "type": "integer",
      "description": "unixtime, The issued time of the token"
    },
    "jwk_url": {
      "type": "string",
      "description": "URL that details the JWT signing"
    },
    "platform": {
      "type": "string",
      "enum": ["Windows 10", "Windows 11", "macOS"],
      "description": "Operating system of the endpoint"
    },
    "serial_number": {
      "type": "string",
      "description": "The serial number of the device derived by unique system
 information"
    },
    "sub": {
      "type": "string",
      "description": "Unique CrowdStrike Agent ID (AID) of machine"
    },
    "typ": {
      "type": "string",
      "enum": ["crowdstrike-zta+jwt"],
      "description": "Generic name for this JWT media. Client MUST reject any other
 type"
    }
  }
}
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par CrowdStrike.

```
permit(principal, action, resource) when {
   context.crowdstrike.assessment.overall > 50
};
```

JumpCloud

JumpCloud est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous la définissez en JumpCloud tant que fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le schéma JSON suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation JumpCloud avec AWS Verified Access, voir Intégration JumpCloud et accès AWS vérifié sur le JumpCloud site Web.

```
{
  "title": "JumpCloud device data specification",
  "type": "object",
  "properties": {
    "device": {
      "type": "object",
      "description": "Properties of the device",
      "properties": {
        "is_managed": {
          "type": "boolean",
          "description": "Boolean to indicate if the device is under management"
        }
      }
    },
    "exp": {
      "type": "integer",
      "description": "Expiration. Unixtime of the token's expiration."
    },
    "durt_id": {
      "type": "string",
      "description": "Device User Refresh Token ID. Unique ID that represents the
 device + user."
```

```
    },
    "iat": {
      "type": "integer",
      "description": "Issued At. Unixtime of the token's issuance."
    },
    "iss": {
      "type": "string",
      "description": "Issuer. This will be 'go.jumpcloud.com'"
    },
    "org_id": {
      "type": "string",
      "description": "The JumpCloud Organization ID"
    },
    "sub": {
      "type": "string",
      "description": "Subject. The managed JumpCloud user ID on the device."
    },
    "system": {
      "type": "string",
      "description": "The JumpCloud system ID"
    }
  }
}
```

Voici un exemple de politique qui évalue par rapport au contexte de confiance fourni par JumpCloud.

```
permit(principal, action, resource) when {
   context.jumpcloud.org_id = 'Unique_orgnaization_identifier'
};
```

Transfert des réclamations de l'utilisateur et vérification des signatures

Une fois qu'une instance d'accès AWS vérifié a authentifié un utilisateur avec succès, elle envoie les demandes d'accès reçues de l'IdP au point de terminaison d'accès vérifié. Les demandes des utilisateurs sont signées afin que les applications puissent vérifier à la fois les signatures et que les demandes ont été envoyées par Verified Access. Au cours de ce processus, l'en-tête HTTP suivant est ajouté :

`x-amzn-ava-user-context`

Cet en-tête contient les revendications de l'utilisateur au format JSON Web Token (JWT). Le format JWT inclut un en-tête, une charge utile et une signature qui sont encodés en URL base64. Verified Access utilise ES384 (algorithme de signature ECDSA utilisant l'algorithme de hachage SHA-384) pour générer la signature JWT.

Les applications peuvent utiliser ces allégations à des fins de personnalisation ou pour d'autres expériences spécifiques aux utilisateurs. Les développeurs d'applications doivent se renseigner sur le niveau d'unicité et de vérification de chaque réclamation fournie par le fournisseur d'identité avant utilisation. En général, la `sub` réclamation est le meilleur moyen d'identifier un utilisateur donné.

Table des matières

Exemple : JWT signé pour les réclamations des utilisateurs de l'OIDC

Les exemples suivants montrent à quoi ressembleront l'en-tête et la charge utile des réclamations des utilisateurs OIDC au format JWT.

Exemple d'en-tête :

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "OIDC Issuer URL"
"exp": "expiration" (120 secs)
}
```

Exemple de charge utile :

```
{
"sub": "xyzsubject",
"email": "xxx@amazon.com",
"email_verified": true,
"groups": [
```

```
"Engineering",
"finance"
]
}
```

Exemple : JWT signé pour les réclamations des utilisateurs d'IAM Identity Center

Les exemples suivants montrent à quoi ressembleront l'en-tête et la charge utile des réclamations des utilisateurs d'IAM Identity Center au format JWT.

> **Note**
>
> Pour IAM Identity Center, seules les informations relatives aux utilisateurs seront incluses dans les réclamations.

Exemple d'en-tête :

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "arn:aws:ec2:us-east-1:123456789012:verified-access-trust-provider/vatp-
abc123xzy321a2b3c",
"exp": "expiration" (120 secs)
}
```

Exemple de charge utile :

```
{
"user": {
        "user_id": "f478d4c8-a001-7064-6ea6-12423523",
        "user_name": "test-123",
        "email": {
            "address": "test@amazon.com",
            "verified": false
        }
    }
```

```
}
```

Clés publiques

Les instances Verified Access ne chiffrant pas les demandes des utilisateurs, nous vous recommandons de configurer les points de terminaison Verified Access pour utiliser le protocole HTTPS. Si vous configurez votre point de terminaison Verified Access pour utiliser le protocole HTTP, veillez à limiter le trafic vers le point de terminaison à l'aide de groupes de sécurité.

Nous vous recommandons de vérifier la signature avant de procéder à toute autorisation sur la base des réclamations. Pour obtenir la clé publique, obtenez l'ID de clé de l'en-tête JWT et utilisez-le pour rechercher la clé publique à partir du point de terminaison. Le point final de chacune d'entre elles Région AWS est le suivant :

`https://public-keys.prod.verified-access.<region>.amazonaws.com/<key-id>`

Exemple : récupération et décodage de JWT

L'exemple de code suivant montre comment obtenir l'ID de clé, la clé publique et la charge utile dans Python 3.9.

```
import jwt
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-ava-user-context']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from Regional endpoint
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
```

```
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES384'])
```

Politiques d'accès vérifiées

AWSLes politiques d'accès vérifié vous permettent de définir des règles d'accès à vos applications hébergées dansAWS. Ils sont rédigés en cèdre, un langage AWS politique. À l'aide de Cedar, vous pouvez créer des politiques qui sont évaluées par rapport au contexte de confiance envoyé par les fournisseurs de confiance basés sur l'identité ou les appareils que vous configurez pour utiliser avec Verified Access.

Pour des informations plus détaillées sur le langage politique de Cedar, consultez le guide de référence de Cedar.

Cette section décrit comment les politiques d'accès vérifié sont structurées, ce qu'elles contiennent, comment les définir, et fournit quelques exemples.

Table des matières

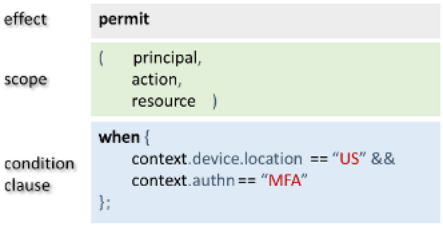
Travaillez avec les politiques d'accès vérifié

Lorsque vous créez un groupe d'accès vérifié ou un point de terminaison d'accès vérifié, vous avez la possibilité de définir la politique d'accès vérifié. Vous pouvez créer un groupe ou un point de terminaison sans définir la politique d'accès vérifié, mais toutes les demandes d'accès seront bloquées jusqu'à ce que vous définissiez une politique.

Pour ajouter ou modifier une politique sur un groupe d'accès vérifié ou un point de terminaison existant après sa création, consultez Modifier une stratégie VAccès VAccès VAccès VAccès VAccès ouModifier une politique de point de terminaison d'accès vérifié.

Structure de la déclaration de politique

Cette section décrit la déclaration de politique d'accès AWS vérifié et la manière dont elle est évaluée. Vous pouvez avoir plusieurs déclarations dans une seule politique d'accès vérifié. Le schéma suivant montre la structure d'une politique d'accès vérifié.



La politique contient les éléments suivants :

- Effet — Spécifie si la déclaration de politique est `permit` (`Allow`) ou `forbid` (`Deny`).
- Champ d'application — Spécifie les principes, les actions et les ressources auxquels l'effet s'applique. Vous pouvez laisser le champ d'application indéfini dans Cedar en n'identifiant pas de principes, d'actions ou de ressources spécifiques (comme indiqué dans l'exemple précédent). Dans ce cas, la politique s'applique à tous les principes, actions et ressources possibles.
- Clause de condition — Spécifie le contexte dans lequel l'effet s'applique.

> **Important**
>
> Pour l'accès vérifié, les politiques sont pleinement exprimées en faisant référence au contexte de confiance dans la clause de condition. Le champ d'application de la politique doit toujours rester indéfini. Vous pouvez ensuite spécifier l'accès en utilisant l'identité et le contexte de confiance de l'appareil dans la clause de condition.

Exemple de politique simple

```
permit(principal,action,resource)
when{
 context.<policy-reference-name>.<attribute> &&
 context.<policy-reference-name>.<attribute2>
};
```

Dans l'exemple précédent, notez que vous pouvez utiliser plusieurs clauses de condition dans une déclaration de politique à l'aide de l'&&opérateur. Le langage politique de Cedar vous donne le pouvoir d'expression nécessaire pour créer des déclarations de politique personnalisées, détaillées et détaillées. Pour accéder à des exemples supplémentaires, consultez Exemples de politiques.

Évaluation des politiques

Un document de politique est un ensemble d'une ou plusieurs déclarations de politique (`permit`ou `forbid` déclarations). La politique s'applique si la clause conditionnelle (la `when` déclaration) est vraie. Pour qu'un document de politique autorise l'accès, au moins une politique d'autorisation du document doit s'appliquer et aucune politique d'interdiction ne peut s'appliquer. Si aucune politique d'autorisation ne s'applique et/ou si une ou plusieurs politiques d'interdiction s'appliquent, le document de politique refuse l'accès. Si vous avez défini des documents de politique pour le groupe Verified Access et le point de terminaison Verified Access, les deux documents doivent autoriser l'accès. Si vous n'avez pas défini de document de politique pour le point de terminaison Verified Access, seule la politique de groupe Verified Access doit y accéder.

> **Note**
>
> AWSVerified Access valide la syntaxe lorsque vous créez la politique, mais il ne valide pas les données que vous avez saisies dans la clause conditionnelle.

Opérateurs intégrés

Lorsque vous créez le contexte d'une politique d'accès AWS vérifié à l'aide de diverses conditions, comme indiqué dansStructure de la déclaration de politique, vous pouvez utiliser l'&&opérateur pour ajouter des conditions supplémentaires. Il existe également de nombreux autres opérateurs intégrés que vous pouvez utiliser pour ajouter un pouvoir d'expression supplémentaire à vos conditions de politique. Le tableau suivant contient tous les opérateurs intégrés à titre de référence.

Opérateur	Types et surcharges	Description
!	Booléen → Booléen	C'est logique, non.
==	n'importe lequel → n'importe quel	Égalité. Fonctionne sur tous les types d'arguments, même

Opérateur	Types et surcharges	Description
		si les types ne correspondent pas. Les valeurs de différent s types ne sont jamais égales entre elles.
!=	n'importe lequel → n'importe quel	Inégalité ; l'exact inverse de l'égalité (voir ci-dessus).
<	(long, long) → booléen	Nombre entier long inférieur à.
<=	(long, long) → booléen	Entier long less-than-or-equal -to.
>	(long, long) → booléen	Nombre entier long supérieur à.
>=	(long, long) → booléen	Entier long greater-than-or-eq ual -to.
dans	(entité, entité) → Booléen	Appartenance à la hiérarchi e (réflexive : A dans A est toujours vrai).
	(entité, ensemble (entité)) → booléen	Appartenance à la hiérarchie : A dans [B, C,...] est vrai si (A et B) || (A dans C) ||... erreur si l'ensemble contient une non-entité.
&&	(booléen, booléen) → booléen	Logique et (court-circuit).
||	(booléen, booléen) → booléen	Logique ou (court-circuit).
.existe ()	entité → Booléen	Existence de l'entité.

Opérateur	Types et surcharges	Description
a	(entité, attribut) → Booléen	Opérateur Infix. `e has f` teste si l'enregistrement ou l'entité `e` possède une liaison pour l'attribut`f`. Renvoie `false` s'il `e` n'existe pas ou s'`e`il existe mais n'a pas l'attribu `tf`. Les attributs peuvent être exprimés sous forme d'identif iants ou de chaînes littérales.
like	(chaîne, chaîne) → Booléen	Opérateur Infix. `t like` pvérifie si le texte `t` correspon d au modèle`p`, qui peut inclure des caractères `*` générique s correspondant à 0 ou plus de n'importe quel caractère . Pour faire correspondre un caractère étoile littéral dans`t`, vous pouvez utiliser la séquence spéciale de caractères échappés `\*` dans`p`.
.contient ()	(ensemble, n'importe lequel) → Booléen	Définissez l'appartenance (B est-il un élément de A).
. Contient tout ()	(set, set) → Booléen	Teste si l'ensemble A contient tous les éléments de l'ensembl e B.
. Contient n'importe quel ()	(set, set) → Booléen	Teste si l'ensemble A contient l'un des éléments de l'ensembl e B.

Commentaires relatifs à la politique

Vous pouvez inclure des déclarations de commentaires dans vos politiques d'accès AWS vérifié. Les commentaires sont définis comme une ligne commençant par une nouvelle ligne `//` et se terminant par une nouvelle ligne.

L'exemple suivant montre les déclarations de commentaires contenues dans la politique.

```
// this policy grants access to users in a given domain with trusted devices
permit(principal, action, resource)
when {
  // the user's email address is in the @example.com domain
  context.idc.user.email.address.contains("@example.com")
  // Jamf thinks the user's computer is low risk or secure.
  && ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

Court-circuitage de la logique des politiques

Vous souhaiterez peut-être rédiger une politique d'accès AWS vérifié qui évalue les données présentes ou non dans un contexte donné. Si vous référencez des données dans un contexte qui n'existe pas, Cedar produira une erreur et évaluera la politique de refus d'accès, quelle que soit votre intention. Par exemple, cela entraînerait un refus, car `fake_provider` cela `bogus_key` n'existe pas dans ce contexte.

```
permit(principal, action, resource) when {
  context.fake_provider.bogus_key > 42
};
```

Pour éviter cette situation, vous pouvez vérifier si une clé est présente à l'aide de l'`has`opérateur. Si l'`has`opérateur renvoie la valeur false, l'évaluation ultérieure de l'instruction chaînée est interrompue et Cedar ne produit aucune erreur en tentant de faire référence à un élément qui n'existe pas.

```
permit(principal, action, resource) when {
  context.identity.user has "some_key" && context.identity.user.some_key > 42
};
```

Cela est particulièrement utile lorsque vous spécifiez une politique qui fait référence à deux fournisseurs de confiance différents.

```
permit(principal, action, resource) when {
  // user is in an allowed group
  context.aws_idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
  &&(
    (
      // if CrowdStrike data is present,
      // permit if CrowdStrike's overall assessment is over 50
      context has "crowdstrike" && context.crowdstrike.assessment.overall > 50
    )
    ||
    (
      // if Jamf data is present,
      // permit if Jamf's risk score is acceptable
      context has "jamf" && ["LOW", "NOT_APPLICABLE", "MEDIUM",
 "SECURE"].contains(context.jamf.risk)
    )
  )
};
```

Exemples de politiques

Exemple 1 : création de politiques pour IAM Identity Center

> **Note**
>
> Comme les noms de groupes peuvent être modifiés, IAM Identity Center fait référence aux groupes en utilisant leur identifiant de groupe. Cela permet d'éviter de violer une déclaration de politique lorsque vous modifiez le nom d'un groupe.

L'exemple de politique suivant autorise l'accès uniquement lorsqu'un utilisateur appartient au `finance` groupe (dont l'ID de groupe est dec242c5b0-6081-1845-6fa8-6e0d9513c107) et possède une adresse e-mail vérifiée.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
};
```

Exemple 1b : ajout de conditions supplémentaires à une déclaration de politique pour IAM Identity Center

L'exemple de politique suivant autorise l'accès uniquement lorsqu'un utilisateur appartient au `finance` groupe (dont l'identifiant de groupe est `dec242c5b0-6081-1845-6fa8-6e0d9513c107`), possède une adresse e-mail vérifiée et le score de risque de l'appareil Jamf est `LOW` égal à.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
    && context.jamf.risk == "LOW"
};
```

Exemple 2 : La même politique pour un fournisseur OIDC tiers

L'exemple de politique suivant autorise l'accès uniquement lorsque l'utilisateur appartient au groupe « finance », qu'il possède une adresse e-mail vérifiée et que le score de risque de l'appareil Jamf est FAIBLE.

```
permit(principal,action,resource)
when {
     context.<policy-reference-name>.groups.contains("finance")
     && context.<policy-reference-name>.email_verified == true
     && context.jamf.risk == "LOW"
};
```

Exemple 3 : utilisation CrowdStrike

L'exemple de politique suivant autorise l'accès lorsque le score d'évaluation global est supérieur à 50.

```
permit(principal,action,resource)
when {
    context.crwd.assessment.overall > 50
};
```

Exemple 4 : utilisation de caractères spéciaux

L'exemple suivant montre comment écrire une politique si une propriété de contexte utilise un `:` (point-virgule), qui est un caractère réservé dans le langage de stratégie.

```
permit(principal, action, resource)
when {
    context.<policy-reference-name>["namespace:groups"].contains("finance")
};
```

Exemple 5 : Autoriser une adresse IP spécifique

L'exemple suivant montre une politique qui n'autorise qu'une adresse IP spécifique.

```
permit(principal, action, resource)
when {
    context.http_request.client_ip == "192.0.2.1"
};
```

Exemple 5a : Bloquer une adresse IP spécifique

L'exemple suivant montre une politique qui bloquera une adresse IP spécifique.

```
forbid(principal,action,resource)
when {
ip(context.http_request.client_ip).isInRange(ip("192.0.2.1/32"))
};
```

Assistant de politique d'accès vérifié

L'assistant de politique d'accès vérifié est un outil de la console d'accès vérifié que vous pouvez utiliser pour tester et développer vos politiques. Il présente la politique du point de terminaison, la stratégie de groupe et le contexte de confiance sur un seul écran, où vous pouvez tester et modifier les politiques.

Les formats de contexte de confiance varient selon les fournisseurs de confiance, et il arrive que l'administrateur de Verified Access ne connaisse pas le format exact utilisé par un certain fournisseur de confiance. C'est pourquoi il peut être très utile de consulter le contexte de confiance et les politiques de groupe et de point de terminaison au même endroit à des fins de test et de développement.

Les sections suivantes décrivent les principes de base de l'utilisation de l'éditeur de politiques.

Tâches

- Étape 1 : Spécifiez vos ressources

Étape 1 : Spécifiez vos ressources

Sur la première page de l'assistant de politique, vous spécifiez le point de terminaison Verified Access avec lequel vous souhaitez travailler. Vous spécifierez également un utilisateur (identifié par adresse e-mail) et, éventuellement, le nom de l'utilisateur et/ou un identifiant d'appareil. Par défaut, la décision d'autorisation la plus récente est extraite des journaux d'accès vérifié pour l'utilisateur spécifié. Vous pouvez éventuellement choisir spécifiquement la décision d'autorisation ou de refus la plus récente.

Enfin, le contexte de confiance, la décision d'autorisation, la politique du point de terminaison et la politique de groupe sont tous affichés sur l'écran suivant.

Pour ouvrir l'assistant de politique et spécifier vos ressources

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Instances d'accès vérifié, puis cliquez sur l'ID d'instance d'accès vérifié pour l'instance avec laquelle vous souhaitez travailler.
3. Choisissez Launch Policy Assistant.
4. Pour Adresse e-mail de l'utilisateur, entrez l'adresse e-mail de l'utilisateur.
5. Pour le point de terminaison d'accès vérifié, sélectionnez le point de terminaison pour lequel vous souhaitez modifier et tester les politiques.
6. (Facultatif) Dans Nom, entrez le nom de l'utilisateur.
7. (Facultatif) Sous Identifiant de l'appareil, indiquez l'identifiant unique de l'appareil.
8. (Facultatif) Pour le résultat de l'autorisation, choisissez le type de résultat d'autorisation récent que vous souhaitez utiliser. Par défaut, le dernier résultat d'autorisation sera utilisé.
9. Choisissez Suivant.

Étape 2 : tester et modifier les politiques

Sur cette page, les informations suivantes vous seront présentées pour travailler :

- Le contexte de confiance envoyé par votre fournisseur de confiance à l'utilisateur et (éventuellement) à l'appareil que vous avez spécifié à l'étape précédente.

- La politique Cedar pour le point de terminaison Verified Access spécifiée à l'étape précédente.
- La politique Cedar pour le groupe d'accès vérifié auquel appartient le point de terminaison.

Les politiques Cedar pour le point de terminaison et le groupe Verified Access peuvent être modifiées sur cette page, mais le contexte de confiance est statique. Vous pouvez désormais utiliser cette page pour consulter le contexte de confiance ainsi que les politiques de Cedar.

Testez les politiques par rapport au contexte de confiance en cliquant sur le bouton Tester les politiques, et le résultat de l'autorisation sera affiché à l'écran. Vous pouvez apporter des modifications aux politiques et retester vos modifications, en répétant le processus si nécessaire.

Une fois que vous êtes satisfait des modifications apportées aux politiques, choisissez Next pour passer à l'écran suivant de l'assistant de stratégie.

Étape 3 : Vérifiez et appliquez les modifications

Sur la dernière page de l'assistant aux politiques, vous verrez les modifications que vous avez apportées aux politiques surlignées pour en faciliter la consultation. Vous pouvez maintenant les consulter une dernière fois et choisir Appliquer les modifications pour valider les modifications.

Vous avez également la possibilité de revenir à la page précédente en choisissant Précédent, ou de vous désinscrire complètement de l'assistant des politiques en choisissant Annuler.

Sécurité en matière d'accès AWS vérifié

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Verified Access, voir AWSServices concernés par programme de conformité AWS .
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Verified Access. Les rubriques suivantes expliquent comment configurer l'accès vérifié pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources d'accès vérifié.

Table des matières

Protection des données dans AWS Verified Access

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans AWS Verified Access. Comme décrit dans ce modèle, AWS est responsable de la protection de

l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Verified Access ou une autre solution Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez

une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement en transit

Verified Access chiffre toutes les données en transit entre les utilisateurs finaux et les points de terminaison Verified Access via Internet à l'aide du protocole TLS (Transport Layer Security) 1.2 ou version ultérieure.

Confidentialité du trafic inter-réseaux

Vous pouvez configurer l'accès vérifié pour restreindre l'accès à des ressources spécifiques de votre VPC. Pour l'authentification basée sur les utilisateurs, vous pouvez également restreindre l'accès à certaines parties de votre réseau, en fonction du groupe d'utilisateurs qui accède aux points de terminaison. Pour plus d'informations, consultez Politiques d'accès vérifiées.

Chiffrement des données au repos pour AWS un accès vérifié

AWSVerified Access chiffre les données au repos par défaut, à l'aide de clés KMS AWS détenues. Lorsque le chiffrement des données au repos est effectué par défaut, cela permet de réduire la charge opérationnelle et la complexité liées à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement. Les sections suivantes expliquent en détail comment Verified Access utilise les clés KMS pour le chiffrement des données au repos.

Table des matières

Accès vérifié et clés KMS

Clés détenues par AWS

Verified Access utilise des clés KMS pour chiffrer automatiquement les informations personnelles identifiables (PII). Cela se produit par défaut, et vous ne pouvez pas vous-même consulter, gérer, utiliser ou auditer l'utilisation des clés détenues par AWS. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez Clés détenues par AWS dans le Guide du développeur AWS Key Management Service.

Bien que vous ne puissiez pas désactiver cette couche de chiffrement ou sélectionner un autre type de chiffrement, vous pouvez ajouter une deuxième couche de chiffrement aux clés de chiffrement AWS détenues existantes en choisissant une clé gérée par le client lorsque vous créez vos ressources d'accès vérifié.

Clés gérées par le client

Verified Access prend en charge l'utilisation de clés symétriques gérées par le client que vous créez et gérez, afin d'ajouter une deuxième couche de chiffrement au chiffrement par défaut existant. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établissement et gestion des politiques IAM et des octrois
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Pour plus d'informations, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service (langue française non garantie).

> **Note**
>
> L'accès vérifié active automatiquement le chiffrement au repos à l'aide de clés AWS détenues pour protéger gratuitement les données personnelles identifiables.

Toutefois, AWS KMS des frais s'appliquent lorsque vous utilisez une clé gérée par le client. Pour plus d'informations sur les tarifs, consultez les AWS Key Management Servicetarifs.

Informations personnelles identifiables

Le tableau suivant résume les informations personnelles identifiables (PII) utilisées par Verified Access et la manière dont elles sont cryptées.

Type de données	AWSchiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
`Trust provider (user-type)` Les fournisseurs de confiance de type utilisateur contiennent des options OIDC telles que AuthorizationEndpoint,, UserInfoEndpoint, ClientId, , ClientSecret, etc., qui sont considérées comme des informations personnelles.	Activées	Activées
`Trust provider (device-type)` Les fournisseurs de confiance de type appareil contiennent un TenantId, qui est considéré comme des informations personnelles.	Activées	Activées
`Group policy` Fourni lors de la création ou de la modification du groupe d'accès vérifié. Contient des règles pour autoriser les	Activées	Activées

Type de données	AWSchiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
demandes d'accès. Peut contenir des informations personnelles telles que le nom d'utilisateur et l'adresse e-mail, etc.		
`Endpoint policy` Fourni lors de la création ou de la modification du point de terminaison Verified Access. Contient des règles pour autoriser les demandes d'accès. Peut contenir des informations personnelles telles que le nom d'utilisateur et l'adresse e-mail, etc.	Activées	Activées

Comment AWS Verified Access utilise les subventions dans AWS KMS

L'accès vérifié nécessite une autorisation pour utiliser votre clé gérée par le client.

Lorsque vous créez des ressources Verified Access chiffrées à l'aide d'une clé gérée par le client, Verified Access crée une subvention en votre nom en envoyant une CreateGrantdemande àAWS KMS. Les subventions AWS KMS sont utilisées pour donner à Verified Access l'accès à une clé gérée par le client dans votre compte.

L'accès vérifié nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez des demandes de déchiffrement AWS KMS à pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour déchiffrer vos données.
- Envoyez RetireGrantdes demandes AWS KMS de suppression d'une subvention.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Dans ce cas, Verified Access ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données.

Utilisation de clés gérées par le client avec accès vérifié

Vous pouvez créer une CMK symétrique à l'aide de la AWS Management Console ou des API AWS KMS. Suivez les étapes de la rubrique Création d'une clé symétrique gérée par le client dans le Guide du développeur AWS Key Management Service.

Politiques clés

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez Gestion de l'accès aux clés gérées par le client dans le Guide du développeur AWS Key Management Service.

Pour utiliser votre clé gérée par le client avec vos ressources d'accès vérifié, les opérations d'API suivantes doivent être autorisées dans la politique des clés :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Accorde un accès de contrôle à une clé KMS spécifiée, ce qui permet d'autoriser les opérations requises par Verified Access. Pour plus d'informations sur l'utilisation des subventions, consultez le guide du AWS Key Management Service développeur.

  Cela permet à Verified Access d'effectuer les opérations suivantes :

  - Appelez `GenerateDataKeyWithoutPlainText` pour générer une clé de données chiffrée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
  - Appelez `Decrypt` pour utiliser la clé de données chiffrée stockée afin d'accéder aux données chiffrées.
  - Configurez un directeur partant à la retraite pour permettre au service de`RetireGrant`.
- `kms:DescribeKey`— Fournit les informations clés gérées par le client pour permettre à Verified Access de valider la clé.
- `kms:GenerateDataKey`— Permet à Verified Access d'utiliser une clé pour chiffrer les données.
- `kms:Decrypt`— Autoriser Verified Access pour déchiffrer les clés de données cryptées.

Voici un exemple de politique clé que vous pouvez utiliser pour l'accès vérifié.

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to use Verified Access",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "verified-access.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
```

```
      ],
      "Resource" : "*"
    }
  ]
```

Pour plus d'informations sur la spécification d'autorisations dans une politique, consultez le Guide du développeur AWS Key Management Service.

Pour plus d'informations sur le dépannage des clés d'accès, consultez le Guide du développeur AWS Key Management Service.

Spécification d'une clé gérée par le client pour les ressources d'accès vérifié

Vous pouvez spécifier une clé gérée par le client afin de fournir un chiffrement de deuxième couche pour les ressources suivantes :

- Groupe d'accès vérifié
- Point de terminaison d'accès vérifié
- Fournisseur de confiance Verified Access

Lorsque vous créez l'une de ces ressources à l'aide deAWS Management Console, vous pouvez spécifier une clé gérée par le client dans la section Chiffrement supplémentaire -- facultatif. Au cours du processus, cochez la case Personnaliser les paramètres de chiffrement (avancés), puis entrez l'ID de AWS KMS clé que vous souhaitez utiliser. Cela peut également être fait lors de la modification d'une ressource existante ou en utilisant leAWS CLI.

> **Note**
>
> Si la clé gérée par le client utilisée pour ajouter un chiffrement supplémentaire à l'une des ressources ci-dessus est perdue, les valeurs de configuration des ressources ne seront plus accessibles. Les ressources peuvent toutefois être modifiées en utilisant le AWS Management Console ou AWS CLI pour appliquer une nouvelle clé gérée par le client et réinitialiser les valeurs de configuration.

AWSContexte de chiffrement de Verified Access

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contiennent des informations contextuelles supplémentaires sur les données. AWS KMS utilise le contexte de

chiffrement en tant que données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

AWSContexte de chiffrement de Verified Access

Verified Access utilise le même contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques, où la clé `aws:verified-access:arn` et la valeur sont le nom de la ressource Amazon Resource Name (ARN). Vous trouverez ci-dessous les contextes de chiffrement pour les ressources d'accès vérifié.

Fournisseur de confiance Verified Access

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessTrustProviderId"
}
```

Groupe d'accès vérifié

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessGroupId"
}
```

Point de terminaison d'accès vérifié

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessEndpointId"
}
```

Pour plus d'informations sur l'utilisation du contexte de chiffrement pour les subventions ou dans les politiques, voir le contexte de chiffrement dans le manuel du AWS Key Management Service développeur.

Surveillance de vos clés de chiffrement pour AWS un accès vérifié

Lorsque vous utilisez une clé KMS gérée par le client avec vos ressources AWS Verified Access, vous pouvez l'utiliser AWS CloudTrailpour suivre les demandes auxquelles Verified Access envoieAWS KMS.

Les exemples suivants sont AWS CloudTrail des événements pour`CreateGrant`,,`RetireGrant`, et `Decrypt` `DescribeKey``GenerateDataKey`, qui surveillent les opérations KMS appelées par Verified Access pour accéder aux données chiffrées par votre clé KMS gérée par le client :

CreateGrant

Lorsque vous utilisez une clé gérée par le client pour chiffrer vos ressources, Verified Access envoie une `CreateGrant` demande en votre nom pour accéder à la clé de votre AWS compte. L'autorisation créée par Verified Access est spécifique à la ressource associée à la clé gérée par le client.

L'exemple d'événement suivant enregistre l'opération `CreateGrant` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
```

```
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
            "encryptionContextSubset": {
                "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-0e54f581e2e5c97a2"
            }
        },
        "granteePrincipal": "verified-access.ca-central-1.amazonaws.com",
        "retiringPrincipal": "verified-access.ca-central-1.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "e5a050fff9893ba1c43f83fddf61e5f9988f579beaadd6d4ad6d1df07df6048f",
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "requestID": "0faa837e-5c69-4189-9736-3957278e6444",
    "eventID": "1b6dd8b8-cbee-4a83-9b9d-d95fa5f6fd08",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
```

```
}
```

RetireGrant

L'accès vérifié utilise l'`RetireGrant`opération pour supprimer une subvention lorsque vous supprimez une ressource.

L'exemple d'événement suivant enregistre l'opération `RetireGrant` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:42:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:47:53Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": null,
    "responseElements": {
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
```

```
    "additionalEventData": {
        "grantId":
 "b35e66f9bacb266cec214fcaa353c9cf750785e28773e61ba6f434d8c5c7632f"
    },
    "requestID": "7d4a31c2-d426-434b-8f86-336532a70462",
    "eventID": "17edc343-f25b-43d4-bbff-150d8fff4cf8",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Verified Access appelle l'`Decrypt`opération pour utiliser la clé de données cryptée stockée afin d'accéder aux données cryptées.

L'exemple d'événement suivant enregistre l'opération `Decrypt` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e",
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "AkK+vi1W/
acBKv7OR8p2DeUrA8EgpTffSrjBqNucODuBYhyZ3hlMuYYJz9x7CwQWZw=="
        }
    },
    "responseElements": null,
    "requestID": "2e920fd3-f2f6-41b2-a5e7-2c2cb6f853a9",
    "eventID": "3329e0a3-bcfb-44cf-9813-8106d6eee31d",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

Verified Access utilise cette `DescribeKey` opération pour vérifier si la clé gérée par le client associée à votre ressource existe dans le compte et dans la région.

L'exemple d'événement suivant enregistre l'opération `DescribeKey` :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "5b127082-6691-48fa-bfb0-4d40e1503636",
    "eventID": "ffcfc2bb-f94b-4c00-b6fb-feac77daff2a",
```

```
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "06535808-7cce-4ae1-ab40-e3afbf158a43",
    "eventID": "1ce79601-5a5e-412c-90b3-978925036526",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Gestion des identités et des accès pour AWS Verified Access

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources d'accès vérifié. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Verified Access.

Utilisateur du service : si vous utilisez le service Verified Access pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'accès vérifié pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Verified Access, consultezRésolution des problèmes liés à l'identité et à l'accès AWS vérifiés.

Administrateur du service — Si vous êtes responsable des ressources d'accès vérifié au sein de votre entreprise, vous avez probablement un accès complet à l'accès vérifié. C'est à vous de déterminer les fonctionnalités et les ressources d'accès vérifié auxquelles les utilisateurs du service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec un accès vérifié, consultezComment fonctionne AWS Verified Access avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Verified Access. Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

Authentification par des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail d'accès AWS. Pour plus d'informations sur la connexion à AWS, consultez Connexion à votre Compte AWSdans le Guide de l'utilisateurConnexion à AWS.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des demandes d'API AWS dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Utilisateur root Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur racine du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est

vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, l'AWS Directory Service, l'annuaire Identity Centerou tout utilisateur qui accède à Services AWS en utilisant des informations d'identification fournies via une source d'identité. Quand des identités fédérées accèdent à Comptes AWS, elles endossent des rôles, ces derniers fournissant des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications et de vos Comptes AWS. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center.
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès interservices : certains Services AWS utilisent des fonctions dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.
  - Sessions de transmission d'accès (FAS) : lorsque vous vous servez d'un utilisateur ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées à Service AWS qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres Services AWS ou ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.
  - Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié au service – Un rôle lié au service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur racine ou séance de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez attacher à plusieurs

utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent les politiques gérées par AWS et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courantes. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder

à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.
- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, consultez Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Comment fonctionne AWS Verified Access avec IAM

Avant d'utiliser IAM pour gérer l'accès à Verified Access, découvrez quelles fonctionnalités IAM sont disponibles avec Verified Access.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Verified Access

Fonction IAM	Support d'accès vérifié
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions de service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de Verified Access et AWS des autres services avec la plupart des fonctionnalités IAM, consultez la section AWSServices compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour l'accès vérifié

Prend en charge les politiques basées sur une identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un Groupes d'utilisateurs IAM ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur

quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, veuillez consulter Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour l'accès vérifié

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

Politiques basées sur les ressources au sein de Verified Access

Prend en charge les politiques basées sur une ressource	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le principal et la ressource se trouvent dans des Comptes AWS différents, un administrateur IAM dans le compte approuvé doit également accorder à l'entité principal (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources

accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour l'accès vérifié

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de politique possèdent généralement le même nom que l'opération d'API AWS associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d'accès vérifié, consultez la section Actions définies par Amazon EC2 dans le Service Authorization Reference.

Les actions de politique dans Verified Access utilisent le préfixe suivant avant l'action :

```
ec2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
    "ec2:action1",
    "ec2:action2"
]
```

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

Ressources relatives aux politiques relatives à l'accès vérifié

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Verified Access et leurs ARN, consultez la section Ressources définies par Amazon EC2 dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon EC2.

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

Clés de conditions de politique pour l'accès vérifié

Prise en charge des clés de condition de stratégie spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition d'accès vérifiées, consultez la section Clés de condition pour Amazon EC2 dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, veuillez consulter Actions définies par Amazon EC2.

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

ACL dans Verified Access

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec accès vérifié

Prend en charge ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés étiquettes. Vous pouvez attacher des étiquettes à des entités IAM (utilisateurs ou rôles), ainsi qu'à de nombreuses ressources AWS. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balise dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec accès vérifié

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les Services AWS qui fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires quand vous vous connectez à la AWS Management Console en utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide d'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour l'accès vérifié

Prend en charge les transmissions de sessions d'accès (FAS)	Oui

Lorsque vous vous servez d'un utilisateur IAM ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées à Service AWS qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres Services AWS ou ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour Verified Access

Prend en charge les fonctions du service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour l'accès vérifié

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés au service Verified Access, consultez. Utiliser des rôles liés à un service pour un accès vérifié

Exemples de politiques basées sur l'identité pour AWS l'accès vérifié

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources d'accès vérifié. Ils ne peuvent pas non plus exécuter des tâches à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Verified Access, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Politique de création d'instances d'accès vérifié

- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources d'accès vérifié dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Démarrer avec AWS gérées et évoluez vers les autorisations de moindre privilège - Pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées AWS qui accordent des autorisations dans de nombreux cas d'utilisation courants. Elles sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des Politiques gérées par le client AWS qui sont spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées via un Service AWS spécifique, comme AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Authentification multifactorielle (MFA) nécessaire : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans votre Compte AWS, activez l'authentification multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Politique de création d'instances d'accès vérifié

Pour créer une instance d'accès vérifié, les principaux IAM doivent ajouter cette déclaration supplémentaire à leur politique IAM.

```
{
    "Effect": "Allow",
    "Action": "verified-access:AllowVerifiedAccess",
    "Resource": "*"
}
```

> **Note**
>
> `verified-access:AllowVerifiedAccess`est une API virtuelle à action uniquement. Il ne prend pas en charge l'autorisation basée sur les ressources, les balises ou les clés de condition. Utilisez une autorisation basée sur une ressource, une balise ou une clé de condition pour l'action de l'`ec2:CreateVerifiedAccessInstance`API.

Exemple de politique pour créer une instance d'accès vérifié. Dans cet exemple, `123456789012` il s'agit du numéro de AWS compte et `us-east-1` de la AWS région.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVerifiedAccessInstance",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "verified-access:AllowVerifiedAccess",
            "Resource": "*"
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Résolution des problèmes liés à l'identité et à l'accès AWS vérifiés

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Verified Access et IAM.

Problèmes

- Je ne suis pas autorisé à effectuer une action dans Verified Access
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources d'accès vérifié

Je ne suis pas autorisé à effectuer une action dans Verified Access

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `ec2:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ec2:`*`GetWidget`*.

Si vous avez encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Verified Access.

Certains Services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer une nouvelle fonction du service ou rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Verified Access. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources d'accès vérifié

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Verified Access prend en charge ces fonctionnalités, consultezComment fonctionne AWS Verified Access avec IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, consultez la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des tiers Comptes AWS, consultez Fournir l'accès aux Comptes AWS appartenant à des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utiliser des rôles liés à un service pour un accès vérifié

AWSVerified Access utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Verified Access. Les rôles liés au service sont prédéfinis par Verified Access et incluent toutes les autorisations dont le service a besoin pour appeler d'autres personnes en votre Services AWS nom.

Un rôle lié à un service facilite la configuration de Verified Access car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Verified Access définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul Verified Access peut assumer ses rôles. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre entité IAM.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour Verified Access

Verified Access utilise le rôle lié au service nommé AWSServiceRoleForVPCVerifiedAccesspour fournir les ressources de votre compte nécessaires à l'utilisation du service.

Le rôle lié à un service AWSServiceRoleForVPCVerifiedAccess approuve les services suivants pour endosser le rôle :

- `verified-access.amazonaws.com`

La politique d'autorisations de rôle, nommée AWSVPCVerifiedAccessServiceRolePolicy, permet à Verified Access d'effectuer les actions suivantes sur les ressources spécifiées :

- Action `ec2:CreateNetworkInterface` sur tous les sous-réseaux et groupes de sécurité, ainsi que sur toutes les interfaces réseau avec le tag `VerifiedAccessManaged=true`
- Action `ec2:CreateTags` sur toutes les interfaces réseau au moment de la création

- Action `ec2:DeleteNetworkInterface` sur toutes les interfaces réseau avec le tag `VerifiedAccessManaged=true`
- Action `ec2:ModifyNetworkInterfaceAttribute` sur tous les groupes de sécurité et toutes les interfaces réseau avec le tag `VerifiedAccessManaged=true`

Vous pouvez également consulter les autorisations relatives à cette politique dans le AWS Management Console AWSVPCVerifiedAccessServiceRolePolicy, ou vous pouvez consulter la AWSVPCVerifiedAccessServiceRolePolicypolitique dans le Guide de référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Verified Access

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous appelez CreateVerifiedAccessEndpointl'AWS Management Console, l'API ou l'AWSAPIAWS CLI, Verified Access crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous appelez à CreateVerifiedAccessEndpointnouveau, Verified Access crée à nouveau le rôle lié au service pour vous.

Modifier un rôle lié à un service pour Verified Access

L'accès vérifié ne vous permet pas de modifier le rôle AWSServiceRoleForVPCVerifiedAccesslié à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Verified Access

Vous n'avez pas besoin de supprimer manuellement le rôle AWSServiceRoleForVPCVerifiedAccess. Lorsque vous appelez DeleteVerifiedAccessEndpointl'AWS Management Console, l'API ou l'AWS CLIAWSAPI, Verified Access nettoie les ressources et supprime le rôle lié au service pour vous.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForVPCVerifiedAccess. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Verified Access

Verified Access prend en charge l'utilisation de rôles liés à un service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez la section AWSRégions et points de terminaison.

AWSpolitiques gérées pour l'accès AWS vérifié

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Politique gérée par AWS : AWSVPCVerifiedAccessServiceRolePolicy

Cette politique est associée à un rôle lié à un service qui permet à Verified Access d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation de rôles liés à un service. Pour consulter les autorisations associées à cette politique, vous pouvez consulter AWSVPCVerifiedAccessServiceRolePolicyleAWS Management Console, ou vous pouvez consulter la AWSVPCVerifiedAccessServiceRolePolicypolitique dans le Guide de référence des politiques AWS gérées.

Accès vérifié : mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour Verified Access depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique des documents d'accès vérifiés.

Modification	Description	Date
AWSVPCVerifiedAccessServiceRolePolicy- Politique mise à jour	Verified Access a mis à jour sa politique de gestion pour inclure des descriptions de toutes les actions dans le champ « sid ».	17 novembre 2023
AWSVPCVerifiedAccessServiceRolePolicy- Politique mise à jour	Verified Access a mis à jour sa politique gérée pour ajouter une ressource de groupe de sécurité à `ec2:CreateNetworkInterface` l'autorisation.	Le 31 mai 2023
AWSVPCVerifiedAccessServiceRolePolicy : nouvelle politique	Verified Access a ajouté une nouvelle politique lui permettant de fournir les ressources nécessaires à l'utilisation du service sur votre compte.	29 novembre 2022
Verified Access a commencé à suivre les modifications	Verified Access a commencé à suivre les modifications apportées AWS à ses politiques gérées.	29 novembre 2022

Validation de conformité pour AWS Verified Access

Accès vérifié par AWSpeut être configuré pour garantir la conformité aux normes fédérales de traitement de l'information (FIPS). Pour plus d'informations et de détails sur la configuration de la conformité FIPS pour Verified Access, rendez-vous sur. Conformité à la norme FIPS pour l'accès vérifié

Pour savoir si un Service AWS fait partie du champ d'application de programmes de conformité spécifiques, consultez Services AWS dans le champ d'application par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides Quick Start de la sécurité et de la conformité : ces guides de déploiement traitent de considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence dans AWS centrés sur la sécurité et la conformité.
- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications éligibles à la loi HIPAA.

  > **Note**
  >
  > Tous les Services AWS ne sont pas éligibles à HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- Guides de conformité destinés aux clients AWS : comprenez le modèle de responsabilité partagée du point de vue de la conformité. Les guides résument les meilleures pratiques pour sécuriser les Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux

cadres (y compris l'Institut national de normalisation et de technologie (NIST), le Conseil de normes de sécurité PCI (Payment Card Industry) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce Service AWS fournit une vue complète de votre état de sécurité dans AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, veuillez consulter Security Hub controls reference (français non garanti).
- AWS Audit Manager – Ce service Service AWS vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience en matière d'accès AWS vérifié

L'infrastructure mondiale d'AWS est construite autour de zones de disponibilité et de Régions AWS. Les Régions AWSfournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Outre l'infrastructure AWS mondiale, Verified Access propose les fonctionnalités suivantes pour répondre à vos besoins en matière de haute disponibilité.

Sous-réseaux multiples pour une haute disponibilité

Lorsque vous créez un point de terminaison Verified Access de type équilibreur de charge, vous pouvez associer plusieurs sous-réseaux au point de terminaison. Chaque sous-réseau que vous associez au point de terminaison doit appartenir à une zone de disponibilité différente. En associant plusieurs sous-réseaux, vous pouvez garantir une haute disponibilité en utilisant plusieurs zones de disponibilité.

Surveillance des accès AWS vérifiés

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et la disponibilité et les performances de AWS Verified Access. AWSfournit les outils de surveillance suivants pour surveiller l'accès vérifié, signaler les incidents et déclencher des actions automatiques le cas échéant :

- Journaux d'accès — Capturez des informations détaillées sur les demandes d'accès aux applications. Pour plus d'informations, veuillez consulter the section called “Journaux d'accès vérifiés”.
- AWS CloudTrail— Capture les appels d'API et les événements associés créés par ou au nom de votre Compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour plus d'informations, veuillez consulter the section called “CloudTrailJournaux ”.

Journaux d'accès vérifiés

Une fois que AWS Verified Access a évalué chaque demande d'accès, il enregistre toutes les tentatives d'accès. Cela fournit une visibilité centralisée sur l'accès aux applications et vous aide à répondre rapidement aux incidents de sécurité et aux demandes d'audit. Verified Access prend en charge le format de journalisation OCSF (Open Cybersecurity Schema Framework).

Lorsque vous activez la journalisation, vous devez configurer une destination pour les journaux à envoyer. Le principal IAM utilisé pour configurer la destination de journalisation devra disposer de certaines autorisations pour que la journalisation fonctionne correctement. Les autorisations IAM requises pour chaque destination de journalisation sont indiquées dans la Autorisations de journalisation section. Verified Access prend en charge les destinations suivantes pour la publication des journaux d'accès :

- Groupes de CloudWatch journaux Amazon Logs
- Compartiments Amazon S3
- Flux de livraison Amazon Data Firehose

Table des matières

- Autorisations de journalisation
- Activer ou désactiver les journaux
- Y compris le contexte de confiance
- Exemples d'entrées de journal pour les journaux d'accès vérifié

Versions de journalisation

Par défaut, le système de journalisation des accès vérifiés utilise la version 0.1 de l'Open Cybersecurity Schema Framework (OCSF). Des exemples de journaux utilisant la version 0.1 peuvent être consultés dans la Exemples d'OCSF version 0.1 section.

La dernière version de journalisation est compatible avec la version OCSF 1.0.0-rc.2. Des détails spécifiques sur le schéma peuvent être trouvés ici Schéma OCSF. Des exemples de journaux utilisant la version 1.0.0-rc.2 peuvent être consultés dans cette section. Exemples de la version 1.0.0-rc.2 d'OCSF

Mettre à jour la version d'enregistrement

Si vous souhaitez mettre à niveau la version de journalisation utilisée, suivez la procédure ci-dessous.

Pour mettre à niveau la version de journalisation à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour mettre à niveau la version de journalisation à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Autorisations de journalisation

Le principal IAM utilisé pour configurer la destination de journalisation devra disposer de certaines autorisations pour que la journalisation fonctionne correctement. Vous trouverez ci-dessous les autorisations requises pour chaque destination de journalisation.

Pour la livraison à CloudWatch Logs :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources
- `logs:DescribeLogGroupslogs:DescribeResourcePolicies`, et `logs:PutResourcePolicy` sur le groupe de journaux de destination

Pour la livraison vers Amazon S3 :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources
- `s3:GetBucketPolicy`et `s3:PutBucketPolicy` sur le compartiment de destination

Pour la livraison à Firehose :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `firehose:TagDeliveryStream`sur toutes les ressources
- `iam:CreateServiceLinkedRole`sur toutes les ressources
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources

Activer ou désactiver les journaux

Lorsque vous activez la journalisation, vous devez configurer une destination pour les journaux à envoyer. Le principal IAM utilisé pour configurer la destination de journalisation devra disposer de certaines autorisations pour que la journalisation fonctionne correctement. Les autorisations IAM requises pour chaque destination de journalisation sont indiquées dans la Autorisations de journalisation section.

Table des matières

Activer les journaux d'accès

Pour activer les journaux d'accès vérifiés à

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. (Facultatif) Pour inclure les données de confiance envoyées par les fournisseurs de confiance dans les journaux, procédez comme suit :
   a. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.
   b. Choisissez Inclure le contexte de confiance.
6. Effectuez l'une des actions suivantes :
   - Activez Deliver to Amazon CloudWatch Logs. Choisissez le groupe de journaux de destination.
   - Activez Deliver to Amazon S3. Entrez le nom, le propriétaire et le préfixe du compartiment de destination.
   - Activez Deliver to Firehose. Choisissez le flux de livraison de destination.
7. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour activer les journaux d'accès vérifiés à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Désactiver les journaux d'accès

Vous pouvez désactiver les journaux d'accès pour votre instance Verified Access à tout moment. Une fois que vous avez désactivé les journaux d'accès, les données de vos journaux restent dans votre destination de journal jusqu'à ce que vous les supprimiez.

Pour désactiver les journaux d'accès vérifiés à

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Désactivez la livraison du journal.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour désactiver les journaux d'accès vérifiés à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Y compris le contexte de confiance

Le contexte de confiance envoyé par votre fournisseur de confiance peut éventuellement être inclus dans vos journaux d'accès vérifié. Cela peut être très utile lorsque vous définissez des politiques qui autorisent ou refusent l'accès à vos applications. Une fois activé, le contexte de confiance se trouve dans le journal situé sous le `data` champ. Si cette option est désactivée, le `data` champ sera défini sur`null`. Pour configurer l'accès vérifié afin d'inclure le contexte de confiance dans les journaux, suivez la procédure ci-dessous.

> **Note**
>
> L'inclusion d'un contexte de confiance dans vos journaux d'accès vérifié nécessite une mise à niveau vers la dernière version de journalisation`ocsf-1.0.0-rc.2`. La procédure ci-

dessous suppose que la journalisation est déjà activée. Si ce n'est pas le cas, consultez Activer les journaux d'accès la procédure complète.

Table des matières

Activer le contexte de confiance

Pour inclure un contexte de confiance dans les journaux d'accès vérifié à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.
6. Activez Inclure le contexte de confiance.
7. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour inclure un contexte de confiance dans les journaux d'accès vérifié à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Désactiver le contexte de confiance

Si vous ne souhaitez plus inclure le contexte de confiance dans les journaux, vous pouvez le supprimer en suivant la procédure ci-dessous.

Pour supprimer le contexte de confiance des journaux d'accès vérifié à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.

4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Désactivez l'option Inclure le contexte de confiance.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour supprimer le contexte de confiance des journaux d'accès vérifié à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Exemples d'entrées de journal pour les journaux d'accès vérifié

Voici des exemples d'entrées de journal.

Table des matières

Exemples d'OCSF version 0.1

Voici des exemples de journaux utilisant la version 0.1 d'OCSF de journalisation par défaut.

Exemples

Accès accordé avec OIDC

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison auprès d'un fournisseur de confiance des utilisateurs OIDC.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
```

```
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
```

```
            "uuid": "00u6wj48lbxTAEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Accès accordé avec OIDC et JAMF

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison auprès des fournisseurs de confiance des appareils OIDC et JAMF.

```
{
    "activity": "Access Granted",
```

```
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0,
        "uid": "41b07859-4222-4f41-f3b9-97dc1EXAMPLE"
    },
    "duration": "0.347",
    "end_time": "1668804944086",
    "time": "1668804944086",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-9778003bc2EXAMPLE"
        },
        "user": {
```

```
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "4f040d0f96becEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-321318ce-6100d340adf4fb29dEXAMPLE",
        "logged_time": 1668805278555,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-18T20:55:44.086480Z",
    "proxy": {
        "ip": "10.5.192.96",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-3598f66575EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "192.168.20.246",
        "port": 61769
    },
    "start_time": "1668804943739",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```


Accès accordé par OIDC et CrowdStrike

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison avec des fournisseurs OIDC et CrowdStrike Device Trust.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.173.3",
        "os": {
            "name": "Windows 11",
            "type": "Windows",
            "type_id": 100
        },
        "type": "Unknown",
        "type_id": 0,
        "uid": "122978434f65093aee5dfbdc0EXAMPLE",
        "hw_info": {
            "serial_number": "751432a1-d504-fd5e-010d-5ed11EXAMPLE"
        }
    },
    "duration": "0.028",
    "end_time": "1668816620842",
    "time": "1668816620842",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "test.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://test.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
```

```
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-506d9753f6EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "23bb45b16a389EXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-c16c5a65-b641e4056cc6cb0eeEXAMPLE",
        "logged_time": 1668816977134,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-19T00:10:20.842295Z",
    "proxy": {
        "ip": "192.168.144.62",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-2f80f37e64EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.14.173.3",
        "port": 55706
    },
    "start_time": "1668816620814",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
```

```
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Accès refusé en raison d'un cookie manquant

Dans cet exemple d'entrée de journal, Verified Access refuse l'accès en raison de l'absence d'un cookie d'authentification.

```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.0",
    "end_time": "1668593568259",
    "time": "1668593568259",
    "http_request": {
        "http_method": "POST",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/dns-query",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/dns-query"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 302
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-5cf1c832-a565309ce20cc7dafEXAMPLE",
        "logged_time": 1668593776720,
        "version": "0.1",
```

```
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T10:12:48.259762Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-108ed7a672EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.7.178.16",
        "port": "46246"
    },
    "start_time": "1668593568258",
    "status_code": "200",
    "status_details": "Authentication Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```


Accès refusé par la politique

Dans cet exemple d'entrée de journal, Verified Access refuse une demande authentifiée car celle-ci n'est pas autorisée par les politiques d'accès.


```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.4.133.137",
        "type": "Unknown",
```

```
        "type_id": 0
    },
    "duration": "0.023",
    "end_time": "1668573630978",
    "time": "1668573630978",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 401
    },
    "identity": {
        "authorizations": [],
        "idp": {
            "name": "user",
            "uid": "vatp-e048b3e0f8EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "0e1281ad3580aEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-531a036a-09e95794c7b96aefbEXAMPLE",
        "logged_time": 1668573773753,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
```

```
    "ref_time": "2022-11-16T04:40:30.978732Z",
    "proxy": {
        "ip": "3.223.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-021d5eaed2EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.4.133.137",
        "port": "31746"
    },
    "start_time": "1668573630955",
    "status_code": "300",
    "status_details": "Authorization Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```


Entrée de journal inconnue

Dans cet exemple d'entrée de journal, Verified Access ne peut pas générer une entrée de journal complète et émet donc une entrée de journal inconnue. Cela garantit que chaque demande apparaît dans le journal d'accès.


```
{
    "activity": "Unknown",
    "activity_id": "0",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.004",
    "end_time": "1668580207898",
    "time": "1668580207898",
    "http_request": {
        "http_method": "GET",
        "url": {
```

```
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-435eb955-6b5a1d529343f5adaEXAMPLE",
        "logged_time": 1668580579147,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:30:07.898344Z",
    "proxy": {
        "ip": "10.1.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-6c32b53b3cEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.28.57.68",
        "port": "47220"
    },
    "start_time": "1668580207893",
    "status_code": "000",
    "status_details": "Unknown",
    "status_id": "0",
    "status": "Unknown",
    "type_uid": "20800100",
    "type_name": "AccessLogs: Unknown",
    "unmapped": null
```

```
}
```

Exemples de la version 1.0.0-rc.2 d'OCSF

Table des matières

Accès accordé avec contexte de confiance inclus

```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
```

```
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
```

```
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": {
        "context": {
            "oidc": {
                "family_name": "Last",
                "zoneinfo": "America/Los_Angeles",
                "exp": 1670631145,
                "middle_name": "Middle",
                "given_name": "First",
                "email_verified": true,
                "name": "Test User Display",
                "updated_at": 1666305953,
                "preferred_username": "johndoe-user@test.com",
                "profile": "http://www.example.com",
                "locale": "US",
                "nickname": "Tester",
                "email": "johndoe-user@test.com"
            },
            "http_request": {
                "x_forwarded_for": "1.1.1.1,2.2.2.2",
                "http_method": "GET",
                "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
                "port": "80",
                "hostname": "hostname.net"
            }
        }
    }
}
```


Accès accordé sans contexte de confiance


```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
```

```
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
```

```
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": null
}
```


Enregistrez les appels de l'API AWS Verified Access à l'aide AWS CloudTrail

AWSL'accès vérifié est intégré àAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un membre Service AWS dans Accès vérifié. CloudTrailenregistre les appels API vers Verified Access sous forme d'événements. Les appels capturés incluent les appels de la console Verified Access et les appels de code adressés aux opérations d'API Verified Access. Si vous créez un journal de suivi, vous pouvez activer la livraison continue d'CloudTrailévénements

à un compartiment Amazon S3, y compris des événements pour Verified Access. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. À l'aide des informations collectées parCloudTrail, vous pouvez déterminer la demande qui a été envoyée à Verified Access, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur de la demande, la date de la demande, ainsi que d'autres informations.

Pour en savoir plus sur CloudTrail, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Informations d'accès vérifiées dans CloudTrail

CloudTrail est activé sur votre Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Accès vérifié, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votreCompte AWS, y compris les événements pour Accès vérifié, créez un journal de suivi. Un journal CloudTrail de suivi permet de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autres Services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions d'accès vérifié sont enregistrées CloudTrail et sont documentées dans la Référence d'API Amazon EC2. Par exemple, les appels adressés aux actions `CreateVerifiedAccessInstance`, `DeleteVerifiedAccessInstance` et `ModifyVerifiedAccessInstance` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour de plus amples informations, veuillez consulter Élément CloudTrail userIdentity.

Se familiariser avec les entrées du fichier journal

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique d'une source quelconque. Il comprend les informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail pour l'action `CreateVerifiedAccessInstance`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIKK4OOINJWEXAMPLE:jdoe",
        "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "jdoe"
    },
    "eventTime": "2022-11-18T20:44:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVerifiedAccessInstance",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
```

```
    "requestParameters": {
        "CreateVerifiedAccessInstanceRequest": {
            "Description": "",
            "ClientToken": "85893b1e-49f6-4d24-97de-280c664edf1b"
        }
    },
    "responseElements": {
        "CreateVerifiedAccessInstanceResponse": {
            "verifiedAccessInstance": {
                "creationTime": "2022-11-18T20:44:04",
                "description": "",
                "verifiedAccessInstanceId": "vai-0d79d91875542c549",
                "verifiedAccessTrustProviderSet": ""
            },
            "requestId": "2eae195d-6bfd-46d7-b46e-a68cb791de09"
        }
    },
    "requestID": "2eae195d-6bfd-46d7-b46e-a68cb791de09",
    "eventID": "297d6529-1144-40f6-abf8-3a76f18d88f0",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Quotas pour AWS un accès vérifié

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre euxService AWS. Sauf indication contraire, chaque quota est spécifique à la région.

Compte AWSquotas de niveau -niveau

Vous Compte AWS disposez des quotas suivants relatifs à l'accès vérifié.

Nom	Par défaut	Ajustable	Description
Instances d'accès vérifiées	5	Oui	Le nombre maximum d'instances à accès vérifié que les clients peuvent créer dans la région actuelle.
Groupes d'accès vérifiés	10	Oui	Le nombre maximum de groupes d'accès vérifiés que les clients peuvent créer dans la région actuelle.
Fournisseurs d'accès sécurisés vérifiés	15	Oui	Le nombre maximum de fournisseurs d'accès sécurisés vérifiés que les clients peuvent créer dans la région actuelle.
Points de terminaison d'accès vérifiés	50	Oui	Le nombre maximum de points de terminaison d'accès vérifiés que les clients peuvent créer dans la région actuelle.

En-têtes HTTP

Les limites de taille pour les en-têtes HTTP sont les suivantes.

Nom	Par défaut	Ajustable
Ligne de demande	16 KM	Non

Nom	Par défaut	Ajustable
En-tête unique	16 KM	Non
En-tête de réponse complet	32 KM	Non
En-tête de demande complet	644 KM	Non

Taille de la réclamation OIDC

Voici la limite de taille des demandes de l'OIDC.

Nom	Par défaut	Ajustable
Taille de la réclamation OIDC	11 KM	Non

Historique des documents pour le guide de l'utilisateur de Verified Access

Le tableau suivant décrit les versions de documentation relatives à Verified Access.

Modification	Description	Date
AWSpolitique gérée mise à jour	Mise à jour apportée à la politique IAM AWS gérée pour Verified Access.	17 novembre 2023
Chiffrement des données au repos	AWSVerified Access chiffre les données au repos par défaut, à l'aide de clés KMS AWS détenues.	28 septembre 2023
Prise en charge de la conformité FIPS	Configurez l'accès vérifié pour la conformité à la norme FIPS.	26 septembre 2023
Journalisation améliorée	Ajout d'une fonctionnalité de journalisation qui ajoute des contextes de confiance aux journaux.	19 juin 2023
AWSpolitique gérée mise à jour	Mise à jour apportée à la politique IAM AWS gérée pour Verified Access.	Le 31 mai 2023
Version GA	Publication générale du guide de l'utilisateur de Verified Access. Inclut AWS WAFl'intégration.	27 avril 2023
Version préliminaire	Version préliminaire du guide de l'utilisateur de Verified Access	29 novembre 2022

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.